VMware™

User's Manual

GSX Server

Version 2.5.1

vmware™

VMware, Inc.

3145 Porter Drive
Palo Alto, CA 94304
www.vmware.com

Please note that you will always find the most up-to-date technical documentation on our Web site at http://www.vmware.com/support/.

The VMware Web site also provides the latest product updates.

Copyright © 2001-2003 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242 and 6,496,847; patents pending. VMware, the VMware "boxes" logo, GSX Server and ESX Server are trademarks of VMware, Inc. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. All other marks and names mentioned herein may be trademarks of their respective companies. Item: GSX-ENG-Q103-009

Table of Contents

Introduction and System Requirements **13**
VMware GSX Server: Enterprise-Class Virtual Machines for Intel-based Servers 14
Welcome to VMware GSX Server 16
Virtualizing Your Computing Resources 17
Host System Requirements 18
Server Requirements 18
Remote Workstation Requirements 22
Virtual Machine Specifications 24
Supported Guest Operating Systems 27
What's New 29
What's New in GSX Server 2.5.1 29
Critical Bug Fixes in Version 2.5.1 30
What's New in GSX Server 2.5 30
Critical Bug Fixes in Version 2.5 32
Technical Support Resources 33
The VMware Web Site 33
VMware Newsgroups 33
Reporting Problems 34

Installing VMware GSX Server **37**
Installing and Uninstalling VMware GSX Server 38
Selecting Your Host System 39
Installing VMware GSX Server on a Windows Host 40
Basic Installation 40
Default Directories 43
Installing the GSX Server Software on a Windows Host 43
About Local and Remote Consoles on the Server 48
Before You Install on a Windows Server 2003 Host 48
Installing VMware GSX Server on a Linux Host 50
Basic Installation 50
Default Directories 53
Installing the GSX Server Software on a Linux Host 53
Installing the VMware Management Interface on a Linux Host 57
About Local and Remote Consoles on the Server 58

Installing an X Server 58
Before You Install on a SuSE Linux 7.1 or Later Host 59
Before You Install on a SuSE Linux Enterprise Server 8 Host 59
Before You Install the VMware Management Interface on a Red Hat Linux 8.0 Host 60
Configuring Internet Explorer 6.0 to Use the VMware Management Interface 61
Launching the Remote Console from the Management Interface on an Encrypted Server 61
Connecting to the Management Interface On a Proxy Server 62
Installing the VMware Remote Console 63
Installing the VMware Remote Console on a Windows Host 63
Installing the VMware Remote Console on a Linux Host 63
Installing the VMware Scripting APIs 65
Installing the VmPerl and VmCOM Scripting APIs on a Windows Host 65
Installing the VmPerl Scripting API on a Linux Host 67
Uninstalling VMware GSX Server 68
Uninstalling GSX Server on a Windows Host 68
Uninstalling GSX Server on a Linux Host 70

Upgrading VMware GSX Server 71
Upgrading VMware GSX Server 72
Preparing for the Upgrade 73
Before You Install GSX Server 73
When You Remove an Existing Version and Install the New Version 74
Upgrading on a Windows Host 75
Upgrading to the Latest Version 75
Upgrading from GSX Server 1 75
Upgrading on a Linux Host 78
Upgrading the Virtual Hardware in Older Windows Guest Operating Systems 80

Creating New Virtual Machines 83
Creating a New Virtual Machine 84
Setting Up a New Virtual Machine on a Windows Host 85
What's in a Virtual Machine on a Windows Host? 85
Simple Steps to a New Virtual Machine on a Windows Host 86
Setting Up a New Virtual Machine on a Linux Host 94
What's in a Virtual Machine on a Linux Host? 94

Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host ____ 96
Simple Steps to a New Virtual Machine on a Linux Host ____ 97
Installing a Guest Operating System ____ 107
Example: Installing Windows 2000 as a Guest Operating System ____ 107

Using VMware Tools ____ 109
Using VMware Tools ____ 110
About VMware Tools ____ 111
Installing VMware Tools ____ 113
Installing VMware Tools in a Windows Virtual Machine ____ 113
Installing VMware Tools in a Linux Virtual Machine ____ 117
Installing VMware Tools in a FreeBSD Virtual Machine ____ 118
Installing VMware Tools in a NetWare Virtual Machine ____ 120
Executing Scripts When the Virtual Machine's Power State Changes ____ 122
Issues to Consider ____ 123
Configuring VMware Tools ____ 124
Configuring VMware Tools in a Windows Virtual Machine ____ 124
Configuring VMware Tools in a Linux or FreeBSD Virtual Machine ____ 128
Configuring VMware Tools in a NetWare Virtual Machine ____ 131
About the VMware Guest Operating System Service ____ 136
Synchronizing the Time in the Guest with the Host Operating System ____ 136
Executing Commands After You Power Off or Reset a Virtual Machine ____ 137
Passing a String from the Host Operating System to the Guest Operating System ____ 137
Passing Information Between the Guest Operating System and a VMware Scripting API Script ____ 140

Managing Virtual Machines ____ 141
Managing Virtual Machines with VMware GSX Server ____ 142
Remotely Managing Virtual Machines ____ 144
Registering the Configuration Files for Virtual Machines ____ 145
Registering a Virtual Machine on a Windows Host ____ 146
Unregistering a Virtual Machine on a Windows Host ____ 146
Registering a Virtual Machine on a Linux Host ____ 147
Unregistering a Virtual Machine on a Linux Host ____ 147
Securing Your Virtual Machines ____ 148

Understanding Permissions in a Running Virtual Machine ____ 148
Authentication and Security Features on a Windows Host ____ 149
Authentication and Security Features on a Linux Host ____ 151
Checking Permissions in the VMware Management Interface ____ 153
Securing Your Remote Sessions ____ 153
Identifying a Virtual Machine by Its UUID ____ 158
Generating the UUID Automatically ____ 158
Comparing the Generated UUID to Configuration File Parameters ____ 159
Setting the UUID for a Virtual Machine that Is Not Being Moved ____ 159
Setting the UUID for a Virtual Machine that Is Being Moved ____ 159
Using the VMware Management Interface ____ 161
Setting the Session Length for the VMware Management Interface ____ 163
Logging In to the VMware Management Interface ____ 163
Using the Status Monitor ____ 165
Viewing Details About a Virtual Machine ____ 171
Downloading Remote Management Packages ____ 175
Creating a New Virtual Machine from the Management Interface ____ 177
Deleting a Virtual Machine Using the VMware Management Interface ____ 181
Configuring the VMware GSX Server Host ____ 182
Logging Out of the VMware Management Interface ____ 182
The Apache Server and the Management Interface ____ 183
Setting a MIME Type to Launch the VMware Remote Console ____ 183

Using Local and Remote Consoles ____ 185
Using Local and Remote Consoles ____ 186
Connecting to Virtual Machines from Local and Remote Consoles ____ 187
How to Run a VMware GSX Server Console ____ 187
Starting the Local Console on a Windows Host ____ 188
Starting the Local Console on a Linux Host ____ 188
Starting the Remote Console on a Windows Remote Workstation ____ 189
Starting the Remote Console on a Linux Remote Workstation ____ 190
Using the Local or Remote Console ____ 191
Powering On Virtual Machines from a Local Console ____ 194
Special Power Options for Virtual Machines ____ 195
Instantly Restoring a Virtual Machine ____ 197
Displaying the Remote Console Banner ____ 198
Changing the Port Number for Remote Console Connections ____ 198
Upgrading the VMware Remote Console ____ 201

Specifying GSX Server Preferences from a Console ____ 207
Setting Input Preferences ____ 207
Setting Hot-Key Preferences ____ 210
Setting Priority Preferences ____ 212
Setting Memory Preferences ____ 214
Setting Workspace Preferences ____ 216
Closing a Console ____ 217

Running Virtual Machines ____ 219
A Quick Guide to Running VMware GSX Server Virtual Machines ____ 220
Displaying Hints ____ 220
Checking the Status of VMware Tools ____ 221
Using Full Screen Mode ____ 222
Installing New Software Inside the Virtual Machine ____ 222
Cutting, Copying and Pasting ____ 223
Sharing Files Between Guest and Host Operating Systems ____ 223
Deciding How Your Virtual Machine Stores Data ____ 228
Suspending and Resuming Virtual Machines ____ 229
Resuming Virtual Machines Repeatedly from the Same Point ____ 231
Shutting Down a Virtual Machine ____ 235
Running Virtual Machines from DVD-ROM or CD-ROM Discs ____ 235
Adding, Configuring and Removing Devices in a Virtual Machine ____ 237
Connecting and Disconnecting Removable Devices ____ 239
Fitting the GSX Server Console Window to the Virtual Machine ____ 239
Creating a Screen Shot of a Virtual Machine ____ 239
Command Reference ____ 240

Moving and Sharing Virtual Machines ____ 241
Moving and Sharing Virtual Machines ____ 242
Moving a Virtual Machine ____ 243
Virtual Machines Use Relative Paths ____ 243
Preparing your Virtual Machine for the Move ____ 244
Moving a Virtual Machine to a New Host Machine ____ 245
Moving an Older Virtual Machine ____ 246
Preparing Your Virtual Machine for the Move ____ 246
Preparing the New Host Machine ____ 247
Considerations for Moving Disks in Undoable Mode ____ 248
Sharing Virtual Machines with Other Users ____ 250

Installing Guest Operating Systems **251**
Choosing and Installing Guest Operating Systems 252
Supported and Unsupported Guest Operating Systems 254
Installation Notes for Particular Guest Operating Systems 256
Windows Server 2003 Installation Guidelines 257
Windows XP Installation Guidelines 260
Windows 2000 Installation Guidelines 263
Windows NT Installation Guidelines 266
Windows Me Installation Guidelines 270
Windows 98 Installation Guidelines 272
Windows 95 Installation Guidelines 275
DOS and Windows 3.1x Installation Notes 280
Mandrake Linux 9.1 Installation Guidelines 282
Mandrake Linux 9.0 Installation Guidelines 284
Mandrake Linux 8.2 Installation Guidelines 286
Mandrake Linux 8.0 and 8.1 Installation Guidelines 288
Red Hat Enterprise Linux 2.1 Installation Guidelines 291
Red Hat Linux 9.0 Installation Guidelines 294
Red Hat Linux 8.0 Installation Guidelines 298
Red Hat Linux 7.3 Installation Guidelines 301
Red Hat Linux 7.1 and 7.2 Installation Guidelines 304
Red Hat Linux 7.0 Installation Guidelines 307
Red Hat Linux 6.x Installation Guidelines 310
SuSE Linux Enterprise Server 8 Installation Guidelines 312
SuSE Linux 8.2 Installation Guidelines 314
SuSE Linux 8.1 Installation Guidelines 316
SuSE Linux 8.0 Installation Guidelines 319
SuSE Linux Enterprise Server 7 Installation Guidelines 322
SuSE Linux 7.3 Installation Guidelines 324
SuSE Linux 7.2 Installation Guidelines 326
SuSE Linux 7.1 Installation Guidelines 328
SuSE Linux 7.0 Installation Guidelines 330
SuSE Linux 6.3 and 6.4 Installation Guidelines 332
SuSE Linux 6.2 Installation Guidelines 334
SuSE Linux 6.1 Installation Guidelines 336
SuSE Linux 6.0 Installation Guidelines 338
Turbolinux 7.0 Installation Guidelines 339
Turbolinux 6.0 Installation Guidelines 341

NetWare 6.0 and 6.5 Server Installation Guidelines ____ 343
NetWare 5.1 Server Installation Guidelines ____ 347
NetWare 4.2 Server Installation Guidelines ____ 351
FreeBSD Installation Guidelines ____ 355

Using Disks ____ 363
Using Disks in a Virtual Machine ____ 364
Configuring Hard Disk Storage in a Virtual Machine ____ 365
Disk Types: Virtual, Raw and Plain ____ 365
Disk Modes: Persistent, Undoable and Nonpersistent ____ 368
Additional Information about Disk, Redo-log and Lock Files ____ 372
Defragmenting and Shrinking Virtual Disks ____ 374
Updating Filenames for Virtual Disks Created with Earlier VMware Products ____ 376
Adding Drives to a Virtual Machine ____ 377
Adding New Virtual Disks to a Virtual Machine ____ 377
Adding Existing Virtual Disks to a Virtual Machine ____ 380
Adding Raw Disks to a Virtual Machine ____ 384
Adding Plain Disks to a Virtual Machine ____ 388
Adding DVD or CD-ROM Drives to a Virtual Machine ____ 392
Adding Floppy Drives to a Virtual Machine ____ 393
Connecting a CD-ROM or Floppy Drive to an Image File ____ 394
Installing an Operating System onto a Raw Partition from a Virtual Machine ____ 396
Configuring a Windows Host ____ 397
Configuring a Linux Host ____ 399
Disk Performance in Windows NT Guests on Multiprocessor Hosts ____ 402
Improving Performance ____ 402

Networking ____ 403
Configuring Your Virtual Network ____ 404
Components of the Virtual Network ____ 406
Common Networking Configurations ____ 408
Bridged Networking ____ 408
Network Address Translation (NAT) ____ 409
Host-Only Networking ____ 411
Custom Networking Configurations ____ 412
Changing the Networking Configuration ____ 415
Adding and Modifying Virtual Network Adapters ____ 415

Configuring Bridged Networking Options on a Windows Host 417
Disabling and Removing NAT and Host-Only Adapters 420
Advanced Networking Topics 423
Selecting IP Addresses on a Host-Only Network or NAT Configuration 423
Avoiding IP Packet Leakage in a Host-Only Network 427
Changing the MAC Address of a Virtual Machine 428
Controlling Routing Information for a Host-Only Network on a Linux Host 429
Other Potential Issues with Host-Only Networking on a Linux Host 429
Using Samba for File Sharing on a Linux Host 431
Configuring a Virtual Machine to Switch Network Adapters on a Windows NT Host 439
Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems 441
Configuring Bridged Networking when Using Teamed Network Interface Cards on Your Host 445
Setting Up a Second Bridged Network Interface on a Linux Host 446
Setting Up Two Separate Host-Only Networks 447
Routing between Two Host-Only Networks 452
Using Virtual Ethernet Adapters in Promiscuous Mode on a Linux Host 457
Understanding NAT 458
Using NAT in GSX Server 458
The Host Computer and the NAT Network 458
DHCP on the NAT Network 459
DNS on the NAT Network 459
External Access from the NAT Network 459
Advanced NAT Configuration 461
Considerations for Using NAT 463
Using NAT with NetLogon (Windows Hosts and Virtual Machines) 464
Sample Windows vmnetnat.conf File 466

Video and Sound 469
Configuring Video and Sound in VMware GSX Server 470
Setting Screen Colors in a Virtual Machine 471
Changing Screen Colors on the Host 471
Changing Screen Colors in the Guest 472
Changing XFree86 Video Resolutions on a Linux Host 473

Configuration 473
Possible Issues 473
Configuring Sound in GSX Server 475
Setting Up Sound in the Guest Operating System 476
Improving Sound Performance 479

Connecting Devices 481
Using Devices with a Virtual Machine 482
Using Parallel Ports 484
Unidirectional Ports 484
Bidirectional Ports 484
Default Configuration 485
Installation in Guest Operating Systems 485
Troubleshooting 488
Configuring a Bidirectional Parallel Port on a Linux Host 488
Devices You Can Use on a Bidirectional Parallel Port 491
Using Serial Ports 492
Using a Serial Port on the Host Computer 492
Using a File on the Host Computer 494
Connecting an Application on the Host to a Virtual Machine 495
Connecting Two Virtual Machines 497
Special Configuration Options for Advanced Users 500
Usage Scenarios: Debugging Over a Virtual Serial Port 501
Keyboard Mapping on a Linux Host 504
Quick Answers 504
The Longer Story 504
V-Scan Code Table 507
Using USB Devices in a Virtual Machine 513
Notes on USB Support 513
Enabling and Disabling the USB Controller 513
Connecting USB Devices 513
Using USB with a Windows Host 514
Using USB with a Linux Host 514
Who Has Control Over a USB Device? 515
Disconnecting USB Devices from a Virtual Machine 516
Human Interface Devices 516
Connecting to a Generic SCSI Device 517
Device Support in Guest Operating Systems 517

Generic SCSI on a Windows Host Operating System 518
Generic SCSI on a Linux Host Operating System 519

Performance Tuning 521
Adjusting Virtual Machines for Best Performance 522
Configuring GSX Server 523
General GSX Server Options 523
GSX Server on a Windows Host 527
GSX Server on a Linux Host 528
Understanding Memory 529
Virtual Machine Memory Size 529
Reserved Memory 530
Using More than 1GB of Memory on a Linux 2.2.x Kernel Host 532
Improving Performance for Guest Operating Systems 534
Windows 2000, Windows XP and Windows Server 2003 Guest Operating System Performance Tips 534
Windows 95 and Windows 98 Guest Operating System Performance Tips 536
Linux Guest Operating System Performance Tips 538

High-Availability Configurations with GSX Server 539
High-Availability Configurations with VMware GSX Server 540
Using SCSI Reservation to Share SCSI Disks With Virtual Machines 541
SCSI Reservation Support 542
Enabling SCSI Reservation 543
Issues to Consider When Sharing Disks 544
Overview of Clustering with GSX Server 546
Applications that Can Use Clustering 547
Clustering Software in Virtual Machines 547
Clustering Scenario: Cluster in a Box 548
Configuring Virtual Machines for Cluster in a Box 549
Creating a Two-Node Cluster with Microsoft Clustering Services on a Single GSX Server Computer 550
Clustering Scenario: Network Load Balancing with GSX Server 557
Overview of Network Load Balancing Clusters 557
Creating a Multinode Network Load Balancing Cluster 558

Glossary 563

Index 569

1

Introduction and System Requirements

VMware GSX Server: Enterprise-Class Virtual Machines for Intel-based Servers

VMware™ GSX Server™ is virtual machine software for Intel-based physical servers.

By isolating operating systems and applications in virtual machines that can co-exist on the same physical server, VMware GSX Server provides better server utilization while ensuring application performance.

When used across servers in production environments, GSX Server provides a virtualization layer that turns your physical computers into a pool of logical computing resources.

This virtualization in turn enables smoother transition between testing, staging and production environments, and dramatic reduction in the cost and complexity of delivering all enterprise services, accelerating return on investment (ROI).

Common Uses of VMware GSX Server

- Implementing server consolidation in software development and test environments and in corporate IT operations
- Delivering high availability of server resources
- Rapid provisioning of server resources
- Streamlining operations at training and demo centers
- Improving effectiveness of software help desk and technical support operations

Because GSX Server allows multiple virtual machines, each with its own operating system, to run at the same time on a single physical machine, it can address a wide range of challenges in the enterprise.

For example, GSX Server is being used at customer locations for rapid development and test, as engineers can rapidly cycle through many environments without physical space or boot time constraints. GSX Server lets customers build clusters using virtual machines to provide the highest levels of availability and software fault tolerance. By supporting clustering of virtual machines, GSX Servermakes high availability both affordable and scalable, reducing hardware and software costs by 30 to 45 percent. Failover is another common application, as one-to-one mirroring of production machines becomes economically feasible when the mirroring machines are virtual machines.

Similarly, systems administrators use the quick-restore, undoable mode virtual disks to upgrade complex software applications or migrate to newer operating systems. Once

the upgrade or migration has been tested for stability, the changes can be committed to the virtual disk — or discarded, if something goes wrong during testing.

VMware GSX Server allows entirely new degrees of functionality within the enterprise.

Key Features of VMware GSX Server

- Server-class performance for enterprise readiness
- Remote management for convenience
- Logical partitioning for improved server utilization, stability and security
- Automation and monitoring for seamless integration
- Uniform platform for hardware independence, flexibility and reliability

With GSX Server, you can economically consolidate applications and infrastructure services onto fewer highly scalable, highly reliable enterprise-class servers.

By using the VMware VmCOM and VmPerl Scripting APIs, you can script common monitoring and management tasks, so the software is easy to integrate into any environment.

With GSX Server, you can remotely manage your servers, individually or as a group, from any location. This cuts server maintenance costs and makes the most efficient use of your IT staff.

Above all, GSX Server lets you deploy services faster and manage server applications and computing resources more easily. The results are optimal flexibility and manageability and much lower total cost of ownership (TCO).

Welcome to VMware GSX Server

This section contains the following:

- Host System Requirements on page 18
- Virtual Machine Specifications on page 24
- Supported Guest Operating Systems on page 27
- What's New on page 29
- Technical Support Resources on page 33

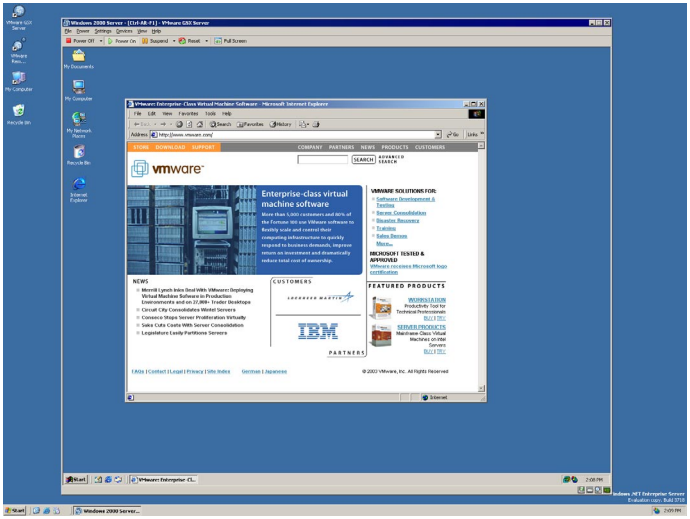
Thank you for choosing VMware GSX Server, the software that increases the productivity of developers and other technical professionals throughout the enterprise by letting them run multiple operating systems in secure, transportable, high-performance virtual computers.

If you're new to GSX Server, this chapter is the place to start. It introduces you to some of the things you can do with GSX Server and guides you through installing the software and putting it to work.

If you're a veteran user of VMware products, take a few minutes to see what's new in version 2 and check out the notes on upgrading your installation.

Virtualizing Your Computing Resources

VMware products provide a virtualization layer that turns your physical computers into a pool of logical computing resources. You can then dynamically allocate those resources to any operating system or application in the way that best meets your needs. You'll be able to spend more time delivering tangible value to your business and less time installing operating systems, rebooting or reconfiguring hardware.



Run the operating systems you need — all at once

With VMware virtualization technology, you can set up completely independent installations of operating systems on a single machine. Multiple instances of Microsoft® Windows® or Linux® can run side by side in virtual machines that you create with the GSX Server software. Each virtual machine is equivalent to a PC with a unique network address and a full complement of hardware devices. You install and run a complete, unmodified operating system and application software, just as you would on a physical PC.

Host and Guest

- The physical computer on which you install the GSX Server software is called the host computer, and its operating system is called the host operating system.
- The operating system running inside a virtual machine is called a guest operating system.
- For definitions of these and other special terms, see the glossary at the end of this manual.

Host System Requirements

What do you need to get the most out of VMware GSX Server? Take the following list of requirements as a starting point. Remember that the virtual machines running under GSX Server are like physical computers in many ways — and, like physical computers, they generally perform better if they have faster processors, more memory and sufficient disk space.

Be aware that system requirements may change after this manual has been printed. For the latest system requirements, go to the VMware Web site at *www.vmware.com/support/gsx25/doc/intro_sysreqs_host_gsx.html*.

Note: VMware GSX Server (for Windows and Linux hosts) is not localized and does not support internationalization. However, virtual machines created with the localized version of VMware Workstation for Windows still work with GSX Server, even though certain elements do not display properly in GSX Server.

Server Requirements

Server Host Hardware

VMware GSX Server supports up to 32-way multiprocessor servers. VMware recommends you run no more than two to four virtual machines concurrently per processor, though you may run a maximum of 64 virtual machines concurrently on a single host.

- Standard x86-based PC or server
- 400MHz or faster processor that supports the Pentium® instruction set

  Compatible processors include

  - Intel®: Pentium II, Pentium III, Pentium III Xeon, Pentium 4, Xeon
  - AMD™: Athlon™, Athlon XP

  Multiprocessor systems supported

Memory

You need enough memory to run the Windows or Linux host operating system plus memory required for each guest operating system and applications on the host and each guest.

- Minimum: 256MB (512MB recommended)
- Maximum: 64GB for Windows hosts and Linux hosts that support large memory or are PAE-enabled; 4GB for non-PAE-enabled Windows hosts; 2GB for Linux hosts with kernels in the 2.2.x series

Display

- Greater than 256-color (8-bit) display adapter required
- Linux hosts must have a video adapter supported by the XFree86 server to run guest operating systems in full screen mode. If an X server is not installed, you must install one, such as XFree86. XFree86 version 3.3.4 or higher is recommended, with XFree86 4.0 preferred.

  SuSE 7.1, 7.2 and 7.3 Hosts Only: You should configure the display settings for the X server on your host to 16-bit color depth to avoid problems with the local and remote consoles having incorrect window dimensions.

Host Hard Disk Requirements

- 275MB free disk space on Windows hosts required for server, VMware Management Interface, VmPerl API, VmCOM API and VMware Remote Console installation (255MB without the remote console)
- 20MB free disk space on Linux hosts required for server, VMware Management Interface, VmPerl API and VMware Remote Console installation
- 20MB free disk space required for VMware Remote Console installation on Windows remote workstation; 10MB required on Linux remote workstation
- At least 1GB free disk space recommended for each guest operating system and the application software used with it; using a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer
- IDE or SCSI hard drives, CD-ROM and DVD-ROM drives supported
- Guest operating systems can boot from raw disk partitions or virtual disk files

Local Area Networking

- Any Ethernet controller supported by the host operating system
- Non-Ethernet networks supported using built-in network address translation (NAT) or using host-only networking plus routing software on the host operating system
- Static IP address for your host machine (recommended)

Software - Windows Host Operating System

You need a Windows **server** operating system with Internet Information Server (IIS) 4.0, 5.0 or 6.0 installed.

- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Standard Edition
- Windows Server 2003 Web Edition
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Advanced Server, including Service Pack 1, Service Pack 2, Service Pack 3 and Service Pack 4
- Microsoft Windows 2000 Server, including Service Pack 1, Service Pack 2, Service Pack 3 and Service Pack 4
- Microsoft Windows NT 4.0 Server, Service Pack 6a with Internet Explorer 5.5 or 6.0 installed (6.0 highly recommended)

In addition, the VMware Management Interface requires one of these browsers:

- Internet Explorer 5.5 or 6.0 (6.0 highly recommended)
- Netscape® Navigator 7.0
- Mozilla 1.x

Note: As newer browser versions are released, VMware tests the management interface for stability and reliability with these versions. We make every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with our product is not supported. For the latest system requirements, go to the VMware Web site at *www.vmware.com/support/gsx25/doc/intro_sysreqs_host_gsx.html*.

Software - Linux Host Operating System

Supported distributions and kernels are listed below. GSX Server may not run on systems that do not meet these requirements.

Note: As newer Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. We make every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the list below, its use with our product is not supported. Look for newer prebuilt modules in the Download area of our Web site. Go to *www.vmware.com/download/*.

- Mandrake™ Linux 9.1 -- stock 2.4.21 kernel
- Mandrake Linux 9.0 -- stock 2.4.19mdk kernel, upgrade 2.4.19-32mdk kernel

- Mandrake Linux 8.2 -- stock 2.4.18-6mdk kernel
- Red Hat™ Enterprise Linux AS 2.1 -- stock 2.4.9-e.3, upgrade 2.4.9-e.16 kernels
- Red Hat Enterprise Linux ES 2.1 -- upgrade 2.4.9-e.16 kernel
- Red Hat Enterprise Linux WS 2.1 -- upgrade 2.4.9-e.16 kernel
- Red Hat Linux 9.0 -- stock 2.4.20-8, upgrade 2.4.20-9 kernels
- Red Hat Linux 8.0 -- stock 2.4.18-14, upgrade 2.4.18-18.8.0, upgrade 2.4.18-27.8.0 kernels
- Red Hat Linux 7.3 -- stock 2.4.18-3, upgrade 2.4.18-18.7.x, upgrade 2.4.18-27-7.x kernels
- Red Hat Linux 7.2 -- stock 2.4.7-10, upgrade 2.4.9-7, upgrade 2.4.9-13, upgrade 2.4.9-21, upgrade 2.4.9-31, upgrade 2.4.18-18.7.x, upgrade 2.4.18-27-7.x kernels
- Red Hat Linux 7.1 -- stock 2.4.2-2, upgrade 2.4.3-12, upgrade 2.4.18-18.7.x upgrade 2.4.18-27-7.x kernels
- Red Hat Linux 7.0 -- stock 2.2.16-22, upgrade 2.2.17-14, upgrade 2.4.18-27-7.x kernels
- SuSE™ Linux Enterprise Server 8 -- stock 2.4.19 kernel

  Caution: Install `gcc` on your SLES 8 host before installing GSX Server. Also, see Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host on page 96 for information on running virtual machines on a SLES 8 host.
- SuSE Linux Enterprise Server 7 -- stock 2.4.7, upgrade 2.4.18 kernels

  Caution: If you intend to upgrade the kernel, make sure you deselect any Samba components when you apply the update patch, as the patch incorrectly updates Samba on your host. Running the update with the Samba packages selected can result in serious issues on your host like system hangs or segmentation faults.
- SuSE Linux 8.2 -- stock 2.4.20 kernel

  Caution: See Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host on page 96 for information on running virtual machines on a SuSE Linux 8.2 host.
- SuSE Linux 8.1 -- upgrade 2.4.19 kernel

  Caution: See Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host on page 96 for information on running virtual machines on a SuSE Linux 8.1 host.
- SuSE Linux 8.0 -- stock 2.4.18 kernel

- SuSE Linux 7.3 -- stock 2.4.10 kernel
- SuSE Linux 7.2 -- stock 2.4.4 kernel
- SuSE Linux 7.1 -- stock 2.2.18, stock 2.4.0 kernels
- SuSE Linux 7.0 -- stock 2.2.16 kernel
- Turbolinux 7.0 -- stock 2.4.5-3 kernel
- Turbolinux 6.0 -- stock 2.2.13-12 kernel

Other Linux host operating system requirements:

- Linux kernel 2.2.14-5.0 is not supported
- Standard Linux **server** installation with `glibc` version 2 or higher and `libXpm.so`
- `inetd` process configured and active for VMware Remote Console and VMware Management Interface connections
- Version 2.1.36 of the SCSI Generic (`sg.o`) driver required to use generic SCSI devices in virtual machines
- Perl 5.005x or higher required to use VmPerl API
- X server required to run the remote console on the server

VmPerl and VmCOM Scripting APIs

The VmPerl API includes the `vmware-cmd` utility. The VmCOM API works on Windows Server 2003, Windows XP, Windows 2000 and Windows NT hosts only. For more information, go to the VMware Web site at *www.vmware.com/support/developer*.

Remote Workstation Requirements

The remote workstation is a Windows NT 4.0 (Workstation or Server), Windows 2000 (Professional, Server, Advanced Server), Windows XP, Windows Server 2003 or Linux system from which you launch the VMware Remote Console to remotely manage a single virtual machine on the GSX Server host. You access the VMware Management Interface to manage multiple virtual machines on the host using a Web browser.

Hardware Requirements

- Standard x86-based computer
- 266MHz or faster processor
- 64MB RAM minimum
- 20MB (Windows hosts), 10MB (Linux hosts) free disk space required for installation of the remote console

Software - Windows Remote Workstation

- Windows Server 2003 Standard edition, Windows Server 2003 Enterprise editionand Windows Server 2003 Web edition
- Windows XP Professional and Windows XP Home Edition, including Service Pack 1
- Windows 2000 Professional, Server and Advanced Server, including Service Pack 1, Service Pack 2, Service Pack 3 and Service Pack 4
- Windows NT 4.0 Workstation and Server, Service Pack 6a
- The VMware Management Interface requires one of these browsers:
  - Internet Explorer 5.5 or 6.0 (6.0 highly recommended)
  - Netscape Navigator 7.0
  - Mozilla 1.x

  Note: As newer browser versions are released, VMware tests the management interface for stability and reliability with these versions. We make every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with our product is not supported. For the latest system requirements, go to the VMware Web site at *www.vmware.com/support/gsx25/doc/intro_sysreqs_host_gsx.html*.

Software - Linux Remote Workstation

Compatible with standard Linux distributions with glibc version 2 or higher and one of the following:

- For single-processor systems: kernel 2.0.32 or higher in the 2.0.x series, or kernel in the 2.2.x series or 2.4.x series (up to and including kernel 2.4.19).
- For SMP systems: kernel in the 2.2.x series or 2.4.x series.

  Note: Linux kernel 2.2.14-5.0 is not supported.
- The VMware Management Interface requires Netscape Navigator 7.0 or Mozilla 1.x.

Virtual Machine Specifications

Each virtual machine created with GSX Server provides a platform that includes the following devices your guest operating system can see.

Processor

- Intel Pentium II or later, depending on host processor
- Single processor per virtual machine on symmetric multiprocessor (SMP) systems

Chip Set

- Intel 440BX-based motherboard with NS338 SIO chip

BIOS

- PhoenixBIOS™ 4.0 Release 6
- DMI/SMBIOS-compliant for system management agent support

Memory

Up to 2000MB of memory per virtual machine, depending upon host operating system, the host system's configuration, the types of applications running on the host and the amount of memory on the host. VMware testing has determined the following memory limits for a virtual machine, based on the host operating system on which the virtual machine is running:

- For Windows Server 2003 and Windows 2000 hosts: up to 1600MB per virtual machine, depending on host memory
- For Linux hosts with kernels in the 2.4.x series: up to 2000MB per virtual machine, depending on host memory
- For Windows NT and Linux hosts with kernels in the 2.2.x series: up to 1300MB per virtual machine, depending on host memory

Graphics

- VGA and SVGA support

IDE Drives

- Up to four devices — disks, CD-ROM or DVD-ROM (DVD drives can be used to read data DVD-ROM discs; DVD video is not supported)
- Hard disks can be virtual disks or physical disks
- IDE virtual disks up to 128GB
- CD-ROM can be a physical device or an ISO image file

SCSI Devices

- Up to 14 devices on 2 virtual SCSI controllers
- SCSI virtual disks up to 256GB
- Hard disks can be virtual disks or physical disks
- Generic SCSI support allows devices to be used without need for drivers in the host operating system; works with scanners, CD-ROM, DVD-ROM, tape drives and other SCSI devices
- Mylex® (BusLogic) BT-958 compatible host bus adapter (requires add-on driver from VMware for Windows XP and Windows Server 2003)

Floppy Drives

- Up to two 1.44MB floppy devices
- Physical drives or floppy image files

Serial (COM) Ports

- Up to four serial (COM) ports
- Output to serial ports, Windows files, Linux files or named pipes

Parallel (LPT) Ports

- Up to two bidirectional parallel (LPT) ports
- Output to parallel ports or host operating system files

USB ports

- Two-port USB 1.1 controller
- Supports devices including USB printers, scanners, PDAs, hard disk drives, memory card readers and still digital cameras

Keyboard

- 104-key Windows 95/98 enhanced

Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablets supported

Ethernet Card

- Up to three virtual Ethernet cards
- AMD PCnet-PCI II compatible

Sound

- Sound output and input
- Creative Labs Sound Blaster® 16, PCM sound compatible (MIDI sound, game controllers and joysticks not supported.)

Virtual Networking and File Sharing

- Nine virtual Ethernet switches (three reserved for bridged, host-only and NAT networking)
- Virtual Ethernet support includes TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell® NetWare® and Network File System
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP and Telnet

Supported Guest Operating Systems

The operating systems listed here have been tested in GSX Server 2 virtual machines and are officially supported. For notes on installing the most common guest operating systems, see Installing Guest Operating Systems on page 251.

Other operating systems designed for Intel-based PCs may work, as well. For a current list of supported guest operating systems, visit the VMware Web site at *www.vmware.com/support/gsx25/doc/intro_sysreqs_guest_gsx.html*.

Microsoft Windows

- Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Editionand Windows Server 2003 Web Edition
- Windows XP Professional and Windows XP Home Edition, including Service Pack 1
- Windows 2000 Professional, Windows 2000 Server and Windows 2000 Advanced Server; Service Pack 3 and Service Pack 4
- Windows NT Workstation 4.0 and Windows NT Server 4.0; Service Pack 3 or higher
- Windows Me
- Windows 98 and Windows 98 SE
- Windows 95 (all OSR releases)
- Windows for Workgroups
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6.22

Linux

- Mandrake Linux 8.0, 8.1, 8.2, 9.0 and 9.1
- Red Hat Linux 6.2, 7.0, 7.1, 7.2, 7.3, 8.0, 9.0 and Red Hat Enterprise Linux (AS, ES, WS) 2.1
- SuSE Linux 6.x, 7.0, 7.1, 7.2, 7.3, 8.0, 8.1, 8.2 and SLES 7, 8
- Turbolinux 6.0 and 7.0

FreeBSD

- FreeBSD 3.x, 4.0, 4.1, 4.2, 4.3, 4.4 and 4.5

Novell NetWare

- NetWare 4.2, 5.1, 6.0 and 6.5

What's New

Here are some highlights of the many new and improved features in this release of VMware GSX Server.

What's New in GSX Server 2.5.1

- Improved reliability of Linux guest installations.
- Improved security, including:
  - Upgrade to OpenSSL 0.9.7.

    GSX Server 2.0 and 2.5.0 use OpenSSL to authenticate and encrypt remote management sessions. Vulnerabilities in the version of the OpenSSL version used by these releases to timing-based man-in-the-middle attacks were reported by OpenSSL.org on February 19, 2003 at *www.openssl.org/news/secadv_20030219.txt*.

    OpenSSL 0.9.7 closes the vulnerabilities to timing-based attacks.
  - SSL used by default for remote management on Linux hosts.

    Security vulnerabilities have been reported in Samba 2.0.x through 2.2.7a. GSX Server for Linux hosts has been upgraded to Samba 2.2.8, which corrects the issue. See *www.kb.cert.org/vuls/id/298233* for details.
  - Upgrade to Samba 2.2.8.
  - Upgrade to Apache 1.3.27.

    This version fixes vulnerabilities listed at *www.apache.org/dist/httpd/Announcement.html*.
- New host and guest operating system support, including:
  - Microsoft Windows Server 2003 host and guest operating system support.
  - Windows 2000 Service Pack 4 host and guest operating system support.
  - Mandrake Linux 9.1 host and guest operating system support.
  - Red Hat Enterprise Linux ES and WS host and guest operating system support.
  - Red Hat Enterprise Linux AS host operating system support with updated kernel.
  - Red Hat Linux 9.0 host and guest operating system support.
  - Red Hat Linux 8.0 update kernel host and guest operating system support. This kernel includes a security patch; for more information, see *cve.mitre.org/cgi-bin/cvename.cgi?name=can-2003-0127*.

- Red Hat Linux 7.x updated kernel. update kernel host and guest operating system support.
- SuSE Linux 8.2 host and guest operating system support.
- SuSE Linux 8.1 update kernel host and guest operating system support. This kernel includes a security patch; for more information, see *cve.mitre.org/cgi-bin/cvename.cgi?name=can-2003-0127*.
- NetWare 6.5 guest operating system support, including VMware Tools.

Critical Bug Fixes in Version 2.5.1

- Fixes for running VMware GSX Server on IBM x440 series machines and hosts with more than 3GB of memory.
- Fixes for running on Stratus ftServer hardware.
- Fix for `vmxnet` networking failure after a soft reboot of the guest operating system. In order to take advantage of the fix, you must reinstall VMware Tools in any Windows guest operating system that uses the `vmxnet` driver. To reinstall VMware Tools, see Installing VMware Tools in a Windows Virtual Machine on page 113.
- Windows 2000 guest operating systems using the `vmxnet` network driver are able to join the domain.

What's New in GSX Server 2.5

- New and faster VMware Management Interface, now with online help. For more information, see Using the VMware Management Interface on page 161.
- Signed Windows networking drivers.
- Improved performance.
  - High-performance `vmxnet` virtual network adapter allows for faster networking performance for Windows Server 2003, Windows XP and Windows 2000 guest operating systems. For more information, see Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems on page 441.
  - Improved SCSI disk performance and boot time for Windows Server 2003, Windows XP and Windows 2000 guest operating systems after you install VMware Tools.
  - Create plain disks — virtual disks where you allocate all of the disk's capacity at creation time for faster disk performance — in the New Virtual Machine

Wizard and the Add Hardware Wizard on a Windows host. For more information, see Adding Plain Disks to a Virtual Machine on page 388.

- Improved clustering support. For more information, see Using SCSI Reservation to Share SCSI Disks With Virtual Machines on page 541.
  - Support for 2 virtual SCSI controllers, doubling the number of SCSI devices available in a virtual machine to 14.
  - Plain disks of up to 128GB in size can be created for faster disk performance and for use in clustered server environments. Plain disks can now be created in the New Virtual Machine Wizard and the Add Hardware Wizard on a Windows host.
- New host and guest operating system support, including:
  - NetWare 6.0, 5.1 and 4.2 guest operating system support, including VMware Tools.
  - Microsoft Windows Server 2003 host and guest operating system support.
  - Microsoft Windows 2000 Datacenter Server host operating system support.
  - Windows 2000 Service Pack 3 host and guest operating system support.
  - Windows XP Service Pack 1 guest operating system support.
  - Mandrake Linux 9.0 host and guest operating system support.
  - Red Hat Linux Advanced Server 2.1 host and guest operating system support.
  - Red Hat Linux 8.0 host and guest operating system support.
  - Red Hat Linux 2.4.18-5 kernel update to Red Hat Linux 7.x and 8.x.
  - SuSE SLES 8 host and guest operating system support.
  - SuSE Linux 8.1 host and guest operating system support.
- Support for larger servers:
  - Up to 64GB host memory support.
  - Up to 32 host processors.
  - Up to 64 running virtual machines on a single VMware GSX Server host.
- Support for PAE-enabled guest operating systems.
- Ability to run a virtual machine from DVD-ROM or CD-ROM. There is no need to copy large virtual disk files from the DVD-ROM or CD-ROM to the VMware GSX Server host. For more information, see Running Virtual Machines from DVD-ROM or CD-ROM Discs on page 235.

- Two-way compatibility when the VMware Remote Console 2.x version differs from the GSX Server 2.x host version; version 2.0 remote consoles can connect to GSX Server 2.5 hosts and version 2.5 remote consoles can connect to GSX Server 2.0 hosts.
- Windows host system-wide configuration settings, including global values for virtual machine memory limits, temp directory location and time synchronization. These settings apply to all virtual machines on a host.

Critical Bug Fixes in Version 2.5

- On systems with fast CPUs, a message that stated the CPU is not recognized by VMware GSX Server no longer appears.
- CGI errors no longer appear when connecting to a Windows Server 2003 or Windows XP host with the VMware Management Interface.
- On a Windows Server 2003 host, resuming a guest operating system with a PAE-enabled kernel no longer returns an internal monitor error.
- On Windows hosts, old VMware network driver files have been removed from the `WINNT\system32\Drivers` directory.
- Ability to launch multiple local consoles on a Linux host has been fixed.
- The VMware Remote Console on a Linux host no longer fails when you set options to automatically power on and off options the virtual machine.
- The installation for a Windows Server 2003 guest operating system no longer hangs.
- Ability to run a Windows Server 2003 guest operating system with more than 256MB of memory.
- When partitioning the virtual disk with a command line disk partitioning tool, the virtual machine no longer crashes with a triple fault error.
- The redo log directory for virtual disks in nonpersistent mode is removed when you reset the virtual machine.
- Linux guest operating systems no longer hang when executing on call instructions.
- The issue with enabling memory limits is fixed. To enable memory limits, see Setting Memory Preferences on page 214.

Technical Support Resources

The VMware Web Site

The latest technical support and troubleshooting notes are available on the VMware Web site at *www.vmware.com/support/*.

VMware's Knowledge Base is another good place to look for answers to questions for and issues with GSX Server. Go to *www.vmware.com/support/kb/enduser/std_alp.php*.

VMware Newsgroups

The VMware newsgroups are primarily forums for users to help each other. You are encouraged to read and post issues, workarounds and fixes. While VMware personnel may read and post to the newsgroups, they are not a channel for official support. The VMware NNTP news server is at *news.vmware.com*.

The following groups are devoted to discussions about GSX Server.
vmware.gsx-server.for-linux
vmware.gsx-server.for-windows
vmware.gsx-server.for-windows.experimental
vmware.remote-mgmt

The following groups are for discussions about guest operating systems.

vmware.guest.linux
vmware.guest.misc
vmware.guest.netware
vmware.guest.windows-nt
vmware.guest.windows2000
vmware.guest.windows95
vmware.guest.windows98
vmware.guest.windowsXP

You can discuss Windows Server 2003 issues in the *vmware.guest.windowsXP* forum.

Reporting Problems

If you have problems while running GSX Server, please report them to the VMware support team.

These guidelines describe the information we need from you to diagnose problems. This information largely comes from various log files. Which log file we need depends upon the problem you encounter.

Be sure to register your serial number. You may then report your problems by submitting a support request at *www.vmware.com/requestsupport*.

Virtual Machine Log File

If a virtual machine exits abnormally or crashes, please save the log file before you launch another virtual machine. The key log file to save is the VMware log file for the affected virtual machine.

On a Windows host, the `vmware.log` file in the same directory as the configuration file (`.vmx`) of the virtual machine that had problems.

On a Linux host, the `<vmname>.log` file in the same directory as the configuration file (`.cfg`) of the virtual machine that had problems.

Also save any core files (`core` or `vmware-core`). Provide these to VMware along with any other information that might help us to reproduce the problem.

Virtual Machine Event Log File

The virtual machine's event log, some of which can be viewed in the VMware Management Interface, is stored as a file on the host. This file can also be useful in the event a virtual machine crashes.

On a Windows host, the file is stored in `C:\Program Files\VMware\VMware GSX Server\vmserverdRoot\eventlog`. Each virtual machine on the host includes an event log file, called `event-<path_to_configuration_file>.vmx.log`.

On a Linux host, the log is called `event-<path_to_configuration_file>.cfg.log` and is stored in `/var/log/vmware`.

VMware Management Interface Log File

The VMware Management Interface keeps a log. If you encounter problems with the management interface, submit this log file along with your support request.

On a Windows host, the log is called `mui.log` and is stored in `C:\Program Files\VMware\VMware Management Interface`.

On a Linux host, the log is called `error_log` and is stored in `/home/vmware/mui/apache/logs`.

VMware Authorization Service Log File

You can enable logging for the VMware Authorization Service manually. If you encounter problems while connecting remotely to a virtual machine on a GSX Server for Windows host, submit this log file along with your support request.

1. In a text editor, open the file `config.ini`, located in `C:\Documents and Settings\All Users\Application Data\VMware\VMware GSX Server`.
2. Add the following lines to the file:
   ```
   vmauthd.logEnabled = TRUE
   log.vmauthdFileName = "C:\authd.log"
   ```
3. Save and close the `config.ini` file.
4. Restart the VMware Authorization Service. Choose **Start** > **Administrative Tools** > **Services**. Right-click the VMware Authorization Service and choose **Restart**.

This enables logging and creates a log file called `authd.log`.

VMware Registration Service Log File

The VMware Registration Service keeps a log. If you encounter problems while connecting to virtual machines or using the management interface, submit this log file along with your support request.

On a Windows host, the log is called `vmware-serverd-SYSTEM-<PID>.log` and is stored in `C:\Windows\Temp` on a Windows Server 2003 or Windows 2000 host. On a Windows NT host, the file is located in `C:\Temp`.

On a Linux host, the log is called `vmware-serverd-<username>-<PID>.log` and is stored in `/tmp`.

VMware GSX Server Installation Log File

If you are reporting a problem you encountered while installing GSX Server, it is helpful to submit your installation log file.

On a Windows host, the file is `VMInst.log`. It is saved in your `temp` folder. On a Windows Server 2003 or Windows 2000 host, the default location is `C:\Documents and Settings\<username>\Local Settings\Temp`. The `Local Settings` folder is hidden by default. To see its contents, open My Computer, go to **Tools** > **Folder Options**, click the **View** tab and select **Show Hidden Files and Folders**. On a Windows NT host, the default location is `C:\Temp`.

On a Linux host, the log is called `locations` and is stored in `/etc/vmware`.

2

Installing VMware GSX Server

Installing and Uninstalling VMware GSX Server

The following sections describe how to install VMware GSX Server on your Windows or Linux host operating system:

- Selecting Your Host System on page 39
- Installing VMware GSX Server on a Windows Host on page 40
  - Basic Installation on page 40
  - Default Directories on page 43
  - Installing the GSX Server Software on a Windows Host on page 43
  - About Local and Remote Consoles on the Server on page 48
  - Before You Install on a Windows Server 2003 Host on page 48
- Installing VMware GSX Server on a Linux Host on page 50
  - Basic Installation on page 50
  - Default Directories on page 53
  - Installing the GSX Server Software on a Linux Host on page 53
  - Installing the VMware Management Interface on a Linux Host on page 57
  - About Local and Remote Consoles on the Server on page 58
  - Installing an X Server on page 58
  - Before You Install on a SuSE Linux 7.1 or Later Host on page 59
  - Before You Install on a SuSE Linux Enterprise Server 8 Host on page 59
  - Before You Install the VMware Management Interface on a Red Hat Linux 8.0 Host on page 60
- Configuring Internet Explorer 6.0 to Use the VMware Management Interface on page 61
- Installing the VMware Remote Console on page 63
  - Installing the VMware Remote Console on a Windows Host on page 63
  - Installing the VMware Remote Console on a Linux Host on page 63
- Installing the VMware Scripting APIs on page 65
  - Installing the VmPerl and VmCOM Scripting APIs on a Windows Host on page 65

    - Installing the VmPerl Scripting API on a Linux Host on page 67
- Uninstalling VMware GSX Server on page 68
    - Uninstalling GSX Server on a Windows Host on page 68
    - Uninstalling GSX Server on a Linux Host on page 70

Selecting Your Host System

VMware GSX Server is available for both Windows and Linux host computers. The installation files for both host platforms are included on the same CD-ROM.

Your serial number allows you to use GSX Server only on the host operating system for which you licensed the software. If you have a serial number for a Windows host, you cannot run the software on a Linux host, and vice versa.

To use GSX Server on a different host operating system — for example, to use it on a Linux host if you have licensed the software for a Windows host — purchase a license on the VMware Web site. You may also request an evaluation license at no charge. For more information, see *www.vmware.com/download/*.

To install on a supported Windows host computer, see Installing VMware GSX Server on a Windows Host on page 40. To install on a Linux host computer, see Installing VMware GSX Server on a Linux Host on page 50.

To review the list of supported host operating systems on which you can install GSX Server, see Host System Requirements on page 18.

Upgrading from Previous Versions

If you are upgrading from a previous version of GSX Server, read Upgrading VMware GSX Server on page 71 before you begin.

Installing VMware GSX Server on a Windows Host

Getting started with GSX Server is simple. The key steps are

1. Install the GSX Server software (including the server, VMware Management Interface, the VmCOM Scripting API, the VmPerl Scripting API and the VMware Remote Console) on the server.
2. Install the VMware Remote Console and VMware Scripting APIs on Windows or Linux workstations.
3. Start the GSX Server local console and enter your serial number. You need to do this only once — the first time you start GSX Server after you install it.
4. Create a virtual machine using the New Virtual Machine Wizard. See Creating New Virtual Machines on page 83.
5. Power on the virtual machine and install a guest operating system. You need the installation media (CD-ROM or floppy disks) for your guest operating system. See Installing a Guest Operating System on page 107.
6. Install the VMware Tools package inside your virtual machine for enhanced performance. See Installing VMware Tools on page 113.
7. Install software in your virtual machine.
8. Start using your virtual machine. Use the VMware Management Interface and VMware Scripting APIs to manage your server host and virtual machines; use the VMware Remote Console to remotely manage a single virtual machine.

Basic Installation

On a Windows host, you install GSX Server from a master installer. The master installer is a convenient way to install all the components of GSX Server — the server software, the VMware Management Interface, the VMware Remote Console and the VMware Scripting APIs — or you can pick and choose which components to install. When you use the master installer, all components are installed in their own directories under one master directory.

A basic installation of GSX Server uses two computers — a server hosting a number of virtual machines and a workstation. The workstation communicates with the virtual machines on the server over a TCP/IP network link.

In more complex installations, one workstation with multiple remote consoles can manage multiple virtual machines on one or more servers. And remote consoles on multiple workstations can connect to any virtual machine on any server.

Before you begin, be sure you have

- A server and host operating system that meet the system requirements for running GSX Server. See Host System Requirements on page 18.
- A remote management workstation and operating system that meet the system requirements for running the GSX Server remote management software. See Remote Workstation Requirements on page 22.
- The GSX Server installation software. If you bought a GSX Server media kit, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is included with the files you downloaded.
- Your GSX Server serial number. The serial number is included in the email message you received from VMware or the reseller from whom you purchased GSX Server.
- The installation CDs or disks for your guest operating systems.
- **(Windows Server 2003 hosts only):** If you plan to use the VMware Management Interface, you must make sure Internet Information Services (IIS) is installed and configured properly. See Before You Install on a Windows Server 2003 Host on page 48.

On the Server

A complete installation on the GSX Server host includes:

- The GSX Server package for the server (which includes the tools needed to create and configure virtual machines and the local console to view and control the virtual machine).
- The VMware Management Interface package (a Web server for managing virtual machines from a browser; for more information, see Managing Virtual Machines on page 141).
- The VMware Remote Console package (to view the virtual machine and allow others to access it at the same time with other remote consoles)
- The VmCOM Scripting API package, a scripting tool that uses COM to manage virtual machines remotely; for more information, go to *www.vmware.com/support/developer.*

- The VmPerl Scripting API package, a scripting tool that uses Perl to manage virtual machines remotely; for more information, go to *www.vmware.com/support/developer.*

You can choose a custom installation path where you install only the packages you need.

In most cases, you work directly at the server when you

- Install the server software.
- Create and configure virtual machines.
- Install the guest operating system and application software in a virtual machine.

On a Workstation

In addition to a Web browser, you can install the following packages on a workstation:

- The VMware Remote Console package.
- The VmPerl and VmCOM Scripting APIs (the VmCOM API can be installed only on a Windows workstation).

These packages are available in the VMware Management Interface and the GSX Server Master Installer (on Windows hosts only). If you are installing the remote console on a Linux host, see Installing the VMware Remote Console on a Linux Host on page 63.

Remote consoles can run on workstations and on the server itself. Remote console packages are available for Windows (Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003) and Linux.

Typically, you run the remote console and browser on a workstation. The browser allows access to the VMware Management Interface. The management interface and remote console let you

- Monitor the operation of a virtual machine.
- Start, stop, reset, suspend and resume a virtual machine.

Essentially, the remote console allows you to remotely manage a single virtual machine, while the management interface allows you to remotely manage the server host and all the virtual machines on the host. Also, you can create and delete virtual machines with the management interface.

The VmPerl and VmCOM APIs can connect to Linux and Windows hosts. However, the VmCOM API can run only on a Windows host or workstation. You can use the APIs to create scripts to automate management of virtual machines and the server host.

Default Directories

By default, the GSX Server components are installed into the following directories:

- The server components are installed in
  `C:\Program Files\VMware\VMware GSX Server`
- The VMware Management Interface components are installed in
  `C:\Program Files\VMware\VMware Management Interface`
- The VMware Remote Console components are installed in
  `C:\Program Files\VMware\VMware Remote Console`
- The VmCOM Scripting API components are installed in
  `C:\Program Files\VMware\VMware VmCOM Scripting API`
- The VmPerl Scripting API components are installed in
  `C:\Program Files\VMware\VMware VmPerl Scripting API`

You can change the directory that contains all the components if you wish, but make note of the new paths you intend to use. The instructions in this manual make use of the default paths.

Installing the GSX Server Software on a Windows Host

You cannot have both VMware GSX Server and VMware Workstation on the same host machine. If you plan to install GSX Server on a host machine that already contains Workstation, you must uninstall the Workstation application first.

If you are upgrading from a previous version of GSX Server, see Upgrading VMware GSX Server on page 71.

1. Log on to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.

   Note: On a Windows Server 2003 host, you must be logged in as a local administrator (that is, not logged in to the domain) in order to install GSX Server.

   Note: Although you must be logged in as an administrator to install GSX Server, a user with normal user privileges can run the program after it is installed.

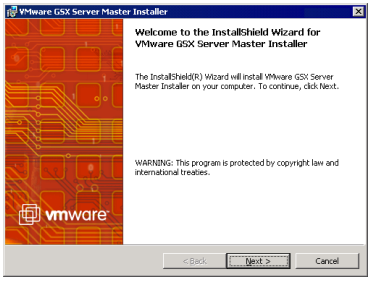
2. Start the GSX Server master installer.

   If you are installing from a CD, from the **Start** menu, choose **Run** and enter `D:\Windows\VMware-gsx-server-installer-<xxxx>.exe`, where `D:` is the drive letter for your CD-ROM drive and `<xxxx>` is a series of numbers representing the version and build numbers.

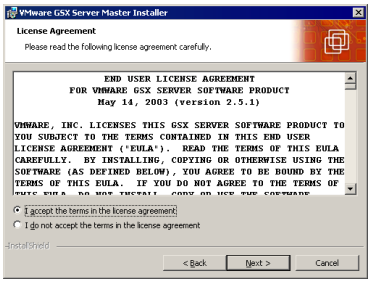
   If you are installing from a downloaded file, from the **Start** menu, choose **Run**, browse to the directory where you saved the downloaded installer file (the

name is similar to `VMware-gsx-server-installer-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers).

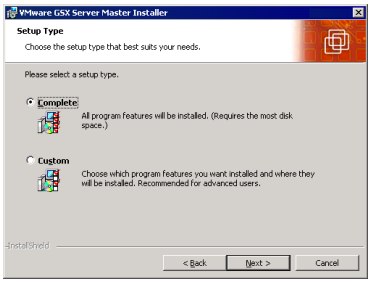
The master installer starts. Click **Next**.


VMware GSX Server Master Installer
Welcome to the InstallShield Wizard for VMware GSX Server Master Installer
The InstallShield(R) Wizard will install VMware GSX Server Master Installer on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
vmware
< Back
Next >
Cancel

3. Acknowledge the end user license agreement (EULA). Select **Yes, I accept the terms in the license agreement**, then click **Next**.


VMware GSX Server Master Installer
License Agreement
Please read the following license agreement carefully.
END USER LICENSE AGREEMENT
FOR VMWARE GSX SERVER SOFTWARE PRODUCT
May 14, 2003 (version 2.5.1)
VMWARE, INC. LICENSES THIS GSX SERVER SOFTWARE PRODUCT TO YOU SUBJECT TO THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT ('EULA'). READ THE TERMS OF THIS EULA CAREFULLY. BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE (AS DEFINED BELOW), YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

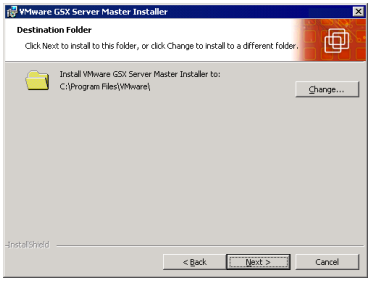
4. Choose whether you want to perform a complete or a custom installation.


VMware GSX Server Master Installer
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

Complete Installation

A complete installation installs the server software, the VMware Management Interface, the VMware Remote Console, the VmPerl Scripting API and the VmCOM Scripting API on the GSX Server host. To choose the complete installation, select **Complete**, then click **Next**.

If you want to install all the GSX Server components in a directory other than the default, click **Change** and browse to the directory of your choice. If the directory does not exist, the installer creates it for you.


VMware GSX Server Master Installer
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install VMware GSX Server Master Installer to:
C:\Program Files\VMware\
Change...
InstallShield
< Back
Next >
Cancel

Caution: GSX Server must be installed on a local drive, not a network drive.

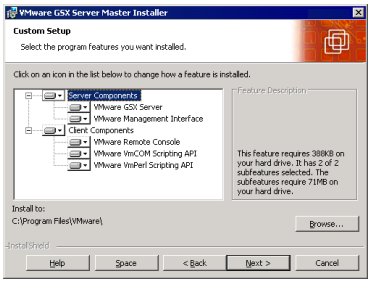
Note: Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive and 240 characters for a path to a folder on a mapped or shared drive. If the path to the GSX Server program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

When you are ready to continue, click **Next** and go to step 5.

Custom Installation

A custom installation lets you pick and choose which components to install. You can always run the installer again at a later date to install components you did not install the first time. Select **Custom** and click **Next**.

In the Custom Setup panel, pick and choose the components to install. Click the arrow to the left of the component you do not want to install and select the appropriate option from the menu.


VMware GSX Server Master Installer
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Server Components
VMware GSX Server
VMware Management Interface
Client Components
VMware Remote Console
VMware VmCOM Scripting API
VMware VmPerl Scripting API
Feature Description
This feature requires 388KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 71MB on your hard drive.
Install to:
C:\Program Files\VMware\
Browse...
InstallShield
Help
Space
< Back
Next >
Cancel

If you need to determine how much free space is on your host click **Space**. This is useful if you are choosing a custom installation due to limited disk space on your host.

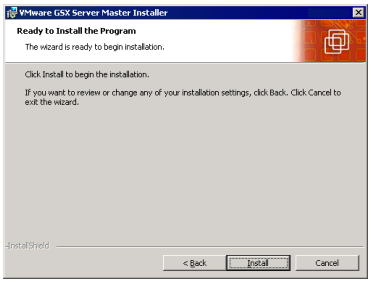
If you want to install all the GSX Server components in a directory other than the default, click **Browse** and select the directory. If the directory does not exist, the installer creates it for you.

Caution: GSX Server must be installed on a local drive, not a network drive.

Note: Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive and 240 characters for a path to a folder on a mapped or shared drive. If the path to the GSX Server program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

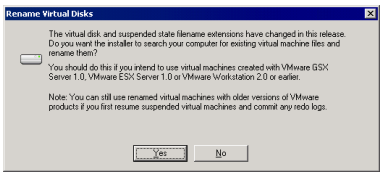
When you are ready to continue, click **Next**.

5. If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the dialog box containing the information you want to change.


VMware GSX Server Master Installer
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

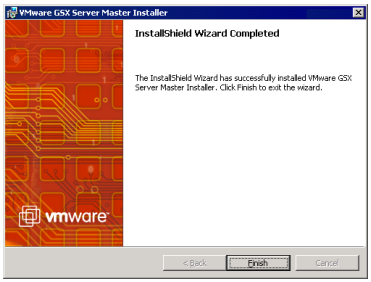
Otherwise, click **Install**. The installer begins copying files to your host.

6. If the installer detects that the CD-ROM autorun feature is enabled, you are prompted with the option to disable it. Disabling this feature prevents undesirable interactions with the virtual machines you install on this system.
7. Two shortcuts are created for you on your desktop automatically, one for the local console (called GSX Server) and one for the VMware Remote Console (provided you installed the remote console). This gives you easy access to virtual machines from the desktop of your host.
8. A dialog box appears, asking if you want to rename existing virtual disks using the `.vmdk` extension (virtual machines created with GSX Server 1.0 or other older VMware products used a `.dsk` extension). Click **Yes** to search all local drives on the host computer and make this change.


Rename Virtual Disks
The virtual disk and suspended state filename extensions have changed in this release. Do you want the installer to search your computer for existing virtual machine files and rename them?
You should do this if you intend to use virtual machines created with VMware GSX Server 1.0, VMware ESX Server 1.0 or VMware Workstation 2.0 or earlier.
Note: You can still use renamed virtual machines with older versions of VMware products if you first resume suspended virtual machines and commit any redo logs.
Yes
No

   The converter also renames the files that store the state of a suspended virtual machine, if it finds them. It changes the old `.std` file extension to `.vmss`. However, it is best to resume and shut down all suspended virtual machines before you upgrade from GSX Server 1 to GSX Server 2.

   Besides renaming files, the converter updates the corresponding virtual machine configuration files so they identify the virtual disks using the new filenames.
9. Click **Finish**. The GSX Server software is installed and you are prompted to reboot the host. Reboot now to start running GSX Server.


VMware GSX Server Master Installer
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed VMware GSX Server Master Installer. Click Finish to exit the wizard.
vmware
< Back
Finish
Cancel

Renaming Disk Files

- The Rename Virtual Disks dialog box appears during installation and the first time you power on a virtual machine. To rename disk files at another time, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 376.

About Local and Remote Consoles on the Server

When you install the server software, a local console and the VMware Remote Console are installed automatically. The local console runs only on the server where the virtual machine is located and is recommended when you need exclusive access to the virtual machine, such as when you install the guest operating system and applications in the virtual machine. The local console runs faster than a remote console (even a remote console on the local host), can utilize full screen mode (for even faster performance), but can only be used when the virtual machine is not connected to by any remote management tools — remote consoles or VMware Scripting APIs. In addition, you cannot perform any power operations on the virtual machine from a browser running the VMware Management Interface.

To run the local console, double-click the VMware GSX Server icon on your desktop.

The remote console lets you manage a virtual machine from the host or remotely from a workstation. It allows other users to connect to this virtual machine at the same time with their own remote consoles and VMware Scripting APIs. Other users can also change the power state of the virtual machine from the management interface.

You should install the remote console on the server as well as at any workstation from which you want to access the virtual machine. This way, you can connect to a virtual machine from the host and give users on other machines the ability to remotely manage this virtual machine at the same time. You can download the remote console from the management interface for an on-the-fly installation on a remote host. For more information, see Downloading Remote Management Packages on page 175.

For more information about consoles, see Using Local and Remote Consoles on page 185.

Before You Install on a Windows Server 2003 Host

Windows Server 2003 does not install Internet Information Services (IIS) by default. You need to install IIS before you can install the VMware Management Interface. To install IIS, in Windows help (choose **Start** > **Help**), then search on the term **IIS**.

Further, Windows Server 2003 only allows the rendering of static Web pages by default, not dynamic pages. In order to render dynamic pages, which are required to display the VMware Management Interface, you need to allow unknown CGI extensions for IIS. To configure IIS to allow unknown CGI extensions, complete the following steps.

1. Choose **Start** > **Administrative Tools** > **Internet Information Services (IIS)**. The Internet Information Services management window opens.

2. Click the + (plus) sign next to the local computer name to expand the components.
3. Click **Web Service Extensions**.
4. In the right window pane, select **All Unknown CGI Extensions**, then click the **Allow** button.
5. Close the Internet Information Services management window.

Installing VMware GSX Server on a Linux Host

Getting started with GSX Server is simple. The key steps are

1. Install the GSX Server software (including the server, VMware Management Interface, the VMware Remote Console and the VmPerl Scripting API) on the server.
2. Install the VMware Remote Console and VMware Scripting APIs on Windows or Linux workstations.
3. Start the GSX Server local console and create a virtual machine using the Configuration Wizard. See Creating New Virtual Machines on page 83.
4. Power on the virtual machine and install a guest operating system. You need the installation media (CD-ROM or floppy disks) for your guest operating system. See Installing a Guest Operating System on page 107.
5. Install the VMware Tools package inside your virtual machine for enhanced performance. See Installing VMware Tools on page 113.
6. Install software in your virtual machine.
7. Start using your virtual machine. Use the VMware Management Interface and VMware Scripting APIs to manage your server host and virtual machines; use the VMware Remote Console to remotely manage a single virtual machine.

Basic Installation

A basic installation of GSX Server uses two computers — a workstation and a server. The workstation communicates with the server over a TCP/IP network link.

In more complex installations, one workstation with multiple remote consoles can manage multiple servers. And remote consoles on multiple workstations can connect to any server.

Before you begin, be sure you have

- A server and host operating system that meet the system requirements for running GSX Server. See Host System Requirements on page 18.
- A remote management workstation and operating system that meet the system requirements for running the GSX Server remote management software. See Remote Workstation Requirements on page 22.
- The installation CDs or disks for your guest operating systems.

- The GSX Server installation software. If you bought a GSX Server media kit, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is in the files you downloaded.
- Your GSX Server serial number. The serial number is included in the email message you received from VMware or the reseller from whom you purchased GSX Server.
- **(SuSE Linux 7.1 and later hosts)**: The `inetd` process configured to start when the host operating system boots. See Before You Install on a SuSE Linux 7.1 or Later Host on page 59.
- **(SuSE Linux Enterprise Server 8 hosts)**: `gcc` installed on your host before you install GSX Server. See Before You Install on a SuSE Linux Enterprise Server 8 Host on page 59.

Caution: Some operating systems, such as Red Hat Linux 7.2 and 7.3, include a firewall by default. This firewall prevents access from remote consoles and the VMware Management Interface to the GSX Server host. In order for the VMware Remote Console to connect to the host, you need to open up port 902. To connect to the host with the VMware Management Interface, you need to open up port 8222. If you are using SSL to make these connections, remember to open up port 443.

On the GSX Server Host Machine

You can install up to four software packages on the Linux server:

- The GSX Server package for the server (from an RPM or tar archive available on the GSX Server CD-ROM or the VMware Web site). The RPM file is called `VMware-gsx-<xxxx>.i386.rpm` while the tar archive is called `VMware-gsx-<xxxx>.tar.gz`, where `<xxxx>` is a series of numbers representing the version and build numbers.
- The VMware Management Interface package (from a tar archive available on the GSX Server CD-ROM or the VMware Web site). This tar archive is called `VMware-mui-<xxxx>.tar.gz`.
- The VMware Remote Console package (from an RPM or tar archive available on the GSX Server CD-ROM, or it can be downloaded from the VMware Web site or the VMware Management Interface). The RPM file is called `VMware-console-<xxxx>.i386.rpm` while the tar archive is called `VMware-console-<xxxx>.tar.gz`.
- The VmPerl Scripting API package, (from a tar archive available on the GSX Server CD-ROM, or it can be downloaded from the VMware Web site or the VMware Management Interface) a scripting tool that uses Perl to manage virtual

machines remotely; for more information, visit the VMware Web site at *www.vmware.com/support/developer.*

In most cases, you work directly at the server when you

- Install the GSX Server software.
- Create and configure virtual machines.
- Install the guest operating system and application software in a virtual machine.

On a Workstation

In addition to a Web browser, you can install the following packages on a workstation:

- The VMware Remote Console package.
- The VmPerl and VmCOM Scripting APIs (the VmCOM API can be installed only on a Windows workstation); for more information, visit the VMware Web site at *www.vmware.com/support/developer.*

These packages are available in the VMware Management Interface. If you are installing the remote console on a Windows host, see Installing the VMware Remote Console on a Windows Host on page 63.

Remote consoles can run on workstations and on the server itself. Remote console packages are available for Windows (Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003) and Linux.

Typically, you run the remote console and browser on a workstation. The browser allows access to the VMware Management Interface. The management interface and remote console let you

- Monitor the operation of a virtual machine.
- Start, stop, reset, suspend and resume a virtual machine.

Essentially, the remote console allows you to remotely manage a single virtual machine, while the management interface allows you to remotely manage the server host and all the virtual machines on the host. Also, you can create and delete virtual machines with the management interface.

The VmPerl and VmCOM APIs can connect to Linux and Windows hosts. However, the VmCOM API can run only on a Windows workstation. You can use the APIs to create scripts to automate management of virtual machines and the server host.

Default Directories

By default, the GSX Server components are installed into the following directories:

- The server components are installed in
  `/usr/bin`
- The VMware Management Interface components are installed in
  `/home/vmware/mui`
- The VMware Remote Console components are installed in
  `/usr/bin`
- The Apache server components are installed in
  `/home/vmware/mui/apache/bin`
  (so they do not conflict with existing Apache software on your server)
- The VmPerl Scripting API executable files are installed in
  `/usr/bin`
- The VmPerl Scripting API library files are installed in
  `/usr/lib/vmware-api`

If you installed the software from a tar installer, you can change these paths if you wish, but make note of the new paths you intend to use. The instructions in this manual make use of the default paths.

Installing the GSX Server Software on a Linux Host

Note: The steps below describe an installation from a CD-ROM disc. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the CD.

You cannot have both VMware GSX Server and VMware Workstation on the same host machine. If you plan to install GSX Server on a host machine that already contains Workstation, the Workstation application is automatically upgraded to GSX Server.

Before you install the GSX Server software, ensure your Linux distribution is for a **server**, not a workstation. If you are running a workstation distribution, you need to install the `inetd` process in order to connect to the VMware Remote Console and VMware Management Interface. If you need to, review the Server Requirements on page 18.

Upgrade Note: If you are upgrading from an earlier version of GSX Server to a later one, the choices you made during the earlier installation become the defaults for the new installation. As a result, you may see options that are different from those described below. For more information, see Upgrading VMware GSX Server on page 71.

1. Log on to your Linux host as the root user.
   `su -`
2. Mount the CD-ROM drive and change to the `Linux` directory on the CD.
   `mount /dev/cdrom /mnt/cdrom`
   `cd /mnt/cdrom/Linux`
3. Do one of the following:
   - If you are installing from the RPM installation package, run the RPM file.
     `rpm -Uhv VMware-gsx-<xxxx>.i386.rpm`
     (where `<xxxx>` is a series of numbers representing the version and build numbers)

     Note: On a Mandrake Linux 8.0 host, you must install GSX Server from a tar package. You cannot install GSX Server from an RPM installer.

     Note: If you are upgrading from GSX Server 1, before you install the RPM package, you need to remove the prebuilt modules RPM package included in the version 1 release. To remove the modules, type the following at a command prompt:
     `rpm -e VMwareGSXKernelModules`
   - To use the tar installer, you may either copy a tar archive to your hard disk and install following the directions below, or skip the steps for copying and unpacking the archive and install directly from the `vmware-gsx-distrib` directory on the CD.

     Caution: Make sure the directory to which you plan to untar the tar archive does not contain any files from a previous GSX Server tar installation.

     Copy the tar archive to a directory on your hard drive, for example, `/tmp`.
     `cp VMware-gsx-<xxxx>.tar.gz /tmp`

     Change to the directory to which you copied the file.
     `cd /tmp`

     Unpack the archive.
     `tar zxf VMware-gsx-<xxxx>.tar.gz`
     (where `<xxxx>` is a series of numbers representing the version and build numbers)

     Change to the installation directory.
     `cd vmware-gsx-distrib`

     Run the installation program.
     `./vmware-install.pl`

Accept the default directories for binary files, library files, manual files, documentation files and `init` script.

4. Run the configuration program.
   `vmware-config.pl`

   Note: If you use the RPM installer, you need to run this program separately from the command line. If you install from the tar archive, the installer offers to launch the configuration program for you. Answer Yes when you see the prompt.

   Use this program to reconfigure GSX Server whenever you upgrade your kernel. It is not necessary to reinstall GSX Server after you upgrade your kernel.

   You can also use `vmware-config.pl` to reconfigure the networking options for GSX Server — for example, to add or remove host-only networks.

5. Press Enter to read the end user license agreement (EULA). You may page through it by pressing the spacebar. If the `Do you accept` prompt does not appear, press Q to get to the next prompt.

6. The remaining prompts are worded in such a way that, in most cases, the default response is appropriate. Further explanation and some exceptions are noted here:

   - To enable host-only networking, respond Yes to the following prompts if they appear:
     ```
     Do you want your virtual machines to be able to use
     the host's network resources?
     Do you want to be able to use host-only networking
     in your virtual machines?
     Do you want this script to probe for an unused
     private subnet?
     ```

     This allows for the sharing of files between the virtual machine and the host operating system. For more information, see Host-Only Networking on page 411.

     Note: If you do not enable host-only networking now, you cannot allow a virtual machine to use both bridged and host-only networking.

     Note: NAT is installed automatically.

   - `Please specify a port for remote console connections to use. [902]` Port 902 is the default port used when you connect to the GSX Server host with the VMware Remote Console. If your site uses this port for another application (for example, *ideafarm-chat* uses this port), then

specify a different port for the remote console to use here. To change the port later, see Changing the Port Number for Remote Console Connections on page 198.

7. If you are upgrading from an earlier version of GSX Server, the following prompt appears: `Do you want the installer to set up permissions for your registered virtual machines? This will be done by setting new permissions on all files found in /etc/vmware/vm-list`.

   Type `y`. The following permissions are set for all registered virtual machines:

   - **Read**, **write** and **execute** — for the user who created the virtual machine (the owner)
   - **Read** and **execute** — for the group
   - **Read** — for users other than the owner or a member of the owner's group

8. Enter your GSX Server serial number exactly as it appears (with hyphens) in the email message you received from VMware or the reseller from whom you purchased GSX Server. When you enter the serial number, it is saved in your license file.

   Note: If you are upgrading from an earlier version with the same major release number (for example, from 2.0 to 2.5), you do not need to enter a serial number.

9. The configuration program displays a message saying the configuration completed successfully. If it does not, run the installation program again.

10. When you finish, do one of the following:

    - Log out of the root account.
      `exit`
    - Install the VMware Management Interface. Go to step 3 under Installing the VMware Management Interface on a Linux Host on page 57.

Installing the VMware Management Interface on a Linux Host

Follow the steps below to install the VMware Management Interface.

Note: If you are installing the management interface on a Red Hat Linux 8.0 host, you must install the `libdb.so.3` library from the Red Hat Linux CD-ROM number 2 first. For more information, see Before You Install the VMware Management Interface on a Red Hat Linux 8.0 Host on page 60.

Note: The steps below describe an installation from a CD-ROM disc. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the CD.

1. In a terminal window, if you haven't done so already, become root so you can carry out the installation.
   ```
   su -
   ```
2. Mount the CD-ROM drive and change to the `Linux` directory on the CD.
   ```
   mount /dev/cdrom /mnt/cdrom
   cd /mnt/cdrom/Linux
   ```
3. Copy the tar archive to a directory on your hard drive, for example, `/tmp`.
   ```
   cp VMware-mui-<xxxx>.tar.gz /tmp
   ```
   (where `<xxxx>` is a series of numbers representing the version and build numbers)

   Caution: Make sure the directory to which you plan to untar the tar archive does not contain any files from a previous VMware Management Interface tar installation.

   Change to the directory to which you copied the file.
   ```
   cd /tmp
   ```

   Unpack the archive.
   ```
   tar zxf VMware-mui-<xxxx>.tar.gz
   ```
   (where `<xxxx>` is a series of numbers representing the version and build numbers)
4. Change to the installation directory.
   ```
   cd vmware-mui-distrib
   ```
5. Run the installation program.
   ```
   ./vmware-install.pl
   ```
6. Press Enter to continue.
7. Accept the EULA.

8. Specify the directory where you want to install the management components. The default is `/home/vmware/mui`.
9. When you finish, you can:
   - Log out of the root account.
     `exit`
   - Install the VMware Remote Console. Go to page 63.
   - Install the VmPerl Scripting API. Go to page 67.

About Local and Remote Consoles on the Server

When you install the server software, a local console is installed automatically. The local console runs only on the server where the virtual machine is located and is recommended when you need exclusive access to the virtual machine, such as when you install the guest operating system and applications in the virtual machine. The local console runs faster than a remote console (even a remote console on the local host), can utilize full screen mode (for even faster performance), but can only be used when the virtual machine is not connected to by any remote management tools — remote consoles or VMware Scripting APIs. In addition, you cannot perform any power operations on the virtual machine from a browser running the VMware Management Interface.

To run the local console, use this command: `vmware -G`.

The VMware Remote Console lets you manage a virtual machine from the host or remotely from a workstation. It allows other users to connect to this virtual machine at the same time with their own remote consoles and VMware Scripting APIs. Other users can also change the power state of the virtual machine from the management interface.

You should install the remote console on the server as well as at any workstation from which you want to access the virtual machine. This way, you can connect to a virtual machine from the host and give users on other machines the ability to remotely manage this virtual machine at the same time. You can download the remote console from the management interface for an on-the-fly installation on a remote host. For more information, see Downloading Remote Management Packages on page 175.

For more information about consoles, see Using Local and Remote Consoles on page 185.

Installing an X Server

You need an X server to run both local and remote consoles. If an X server is not installed, you must install `libxpm.so.4`, located on your Linux distribution disk.

Before You Install on a SuSE Linux 7.1 or Later Host

The `inetd` process, which is required for the VMware Management Interface and remote consoles to run properly, is not configured to start at boot time on SuSE Linux 7.1, 7.2, 7.3, 8.0 and 8.1 hosts.

Before you install GSX Server on a SuSE Linux 7.1 or later host system, you need to configure your SuSE Linux 7.1 or later host so that the `inetd` process starts at boot time. Boot the host operating system and make sure the network card and disk subsystem work as expected.

Configuring the inetd Process in the Host Operating System

1. Start your X server, if it does not start by default, and log in as the root user.
2. Run YAST2, the default configuration utility for SuSE Linux 7.2 and later.
3. Click **Network** (SuSE Linux 7.1) or **Network/Basic** (SuSE Linux 7.2 or later), then click **Start/stop services (inetd)**.
4. Select the **On with default configuration** option.
5. Click **Finish**, then click **Close** to exit YAST2. The `inetd` process automatically starts when you reboot the host operating system.

Before You Install on a SuSE Linux Enterprise Server 8 Host

The `gcc` program is not installed on a SLES 8 host by default. This compiler is required by the VmPerl Scripting API.

Before you install GSX Server on a SLES 8 host system, you must install `gcc`.

Installing gcc in the Host Operating System

1. Start your X server, if it does not start by default, and log in as the root user.
2. Run YAST2, the default configuration utility for SLES 8.
3. Click **Software** in the left pane, click **Install or remove software** in the right pane.
4. Check **C++ Compiler and Tools** in the left pane, then click **Accept**.
5. When prompted, insert the SLES 8 CD.
6. Click **Close** to exit YAST2. The `gcc` program is installed and you can install GSX Server.

Before You Install the VMware Management Interface on a Red Hat Linux 8.0 Host

If you are running GSX Server on a Red Hat Linux 8.0 host, you must install the `libdb.so.3` library from the Red Hat Linux CD-ROM number 2 before you install the VMware Management Interface. The version that comes with the default Red Hat Linux installation is incompatible with the management interface and returns the following error when you start the management interface:

```
Couldn't find necessary components on your system. It
appears that you are missing the following library:
libdb.so.3.

New versions of Red Hat Linux (8.0+) are known to ship
without these libraries. If you are running Red Hat 8.0 or
greater, please install this rpm: compat-db-3.3-<###> rpm
(where <###> is a version number particular to your
version of the distribution from your installation CD.

If you are running a distribution other than Red Hat,
please contact your vendor for a suitable library. Once
the package has been installed, you may start the
$PRODUCTNAME with the following command:

/home/vmware/mui/apache/bin/apachectl/start
```

To install the correct library, run the `compat-db-3.3.<###>.i386.rpm` RPM package. If you installed this package after you installed the management interface software, you can start the management interface with the following command:

```
/etc/init.d/httpd.vmware start
```

Configuring Internet Explorer 6.0 to Use the VMware Management Interface

If you intend to run the VMware Management Interface in Internet Explorer 6.0 on a Windows system, you must take certain steps to configure Internet Explorer properly. These steps are needed whether the browser is running on a GSX Server Windows host or you are using a Windows client machine to connect to a GSX Server host.

The configuration steps allow you to perform the following activities:

- Launching the Remote Console from the Management Interface on an Encrypted Server on page 61
- Connecting to the Management Interface On a Proxy Server on page 62

Launching the Remote Console from the Management Interface on an Encrypted Server

You can launch the VMware Remote Console from the VMware Management Interface automatically. In order to do this in an Internet Explorer 6.0 browser on a Windows system where SSL is encrypting your GSX Server remote connections, you must ensure that the **Do not save encrypted pages to disk** option is disabled.

For information on encrypting remote connections, see Securing Your Remote Sessions on page 153.

When this option is enabled, Internet Explorer does not save any files to disk, including the files it needs to hand off to helper applications. This prevents the remote console from launching automatically.

Caution: This option may have been enabled deliberately at your site to prevent the saving of sensitive files to disk. Disabling it may permit other sensitive information to be saved to disk.

To disable the option, complete the following steps.

1. In the Internet Explorer 6.0 window, open the Internet Options control panel. Choose **Tools** > **Internet Options**.
2. Click the **Advanced** tab.
3. Scroll down to the Security section and uncheck **Do not save encrypted pages to disk**.
4. Click **OK**.

Connecting to the Management Interface On a Proxy Server

If your network is protected behind a proxy server, there are certain steps you must take in order to use the management interface in Internet Explorer 6.0 on a Windows system. Follow the steps for the appropriate Windows operating system.

Windows Server 2003 Systems

1. Launch Internet Explorer 6.0.
2. Choose **Tools** > **Internet Options**, then click the **Security** tab.
3. Select **Trusted sites**, then click **Sites**.
4. In the **Add this Web site to the zone** entry field, type `https://*.domain.com`
5. Click **Add**.
6. Click **OK** until you return to the browser window.

When you use Internet Explorer 6.0 to connect to the management interface, be sure to use fully qualified domain names.

Windows Systems Other than Windows Server 2003

Follow these steps for Windows 2000, Windows XP and Windows NT operating systems.

1. Launch Internet Explorer 6.0.
2. Choose **Tools** > **Internet Options**.
3. Click the **Connections** tab, then click **LAN Settings**.
4. Make sure that **Bypass proxy server for local addresses** is checked.
5. Click **OK** until you return to the browser window.

When you use Internet Explorer 6.0 to connect to the management interface, do **not** use fully qualified domain names.

Connecting to the Management Interface when there Is No Proxy Server

If you are on a Windows system and your network does not use a proxy server, you must use fully-qualified domain names when connecting to the management interface with Internet Explorer 6.0.

Installing the VMware Remote Console

The VMware Remote Console software package enables you to view and control a GSX Server virtual machine from a remote workstation or on the server host. Multiple users can use the remote console to connect to a virtual machine from the server host or from remote workstations at the same time. Use the instructions below that correspond to the operating system running on your system.

Remote consoles can also be launched from the VMware Management Interface. If you use Netscape or Mozilla as your browser, you need to configure the MIME type for the remote console. To set the MIME type, see Setting a MIME Type to Launch the VMware Remote Console on page 183. Internet Explorer is automatically configured when you install the console software.

Installing the VMware Remote Console on a Windows Host

On the GSX Server for Windows host, the VMware Remote Console is installed automatically from the master installer if you chose a complete installation. You can use the master installer to install just the remote console on a remote workstation. To install the remote console from the master installer, see Installing the Remote Console from the GSX Server Master Installer on page 204.

In addition, you can download the remote console from the download menu on the Login page of the VMware Management Interface. To download and install the remote console from the management interface, see Downloading and Installing the VMware Remote Console from the VMware Management Interface on page 202.

Installing the VMware Remote Console on a Linux Host

You can install the VMware Remote Console from the GSX Server CD-ROM or from a file you download from the VMware Web site or from the download menu on the Login page of the VMware Management Interface. Complete the following steps to install the remote console.

Note: The steps below describe an installation from a CD-ROM disc. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the CD.

1. In a terminal window, if you have not done so already, become root so you can carry out the installation steps.

   ```
   su -
   ```

2. Mount the CD-ROM drive and change to the `Linux` directory on the CD.
   ```
   mount /dev/cdrom /mnt/cdrom
   cd /mnt/cdrom/Linux
   ```
3. Unzip the client installer archive to `/tmp`.
   ```
   unzip VMware-gsx-server-linux-client-<xxxx>.zip -d
   /tmp
   ```
   (where <xxxx> is a series of numbers representing the version and build numbers)

   Caution: If you intend to install the VMware Remote Console from a tar package, make sure the directory to which you plan to untar the tar archive does not contain any files from a previous remote console tar installation.
4. Change to the `/tmp` directory.
   ```
   cd /tmp
   ```
5. Do one of the following:
   - If you are installing from the RPM installation package, run the RPM file.
     ```
     rpm -Uhv VMware-console-<xxxx>.i386.rpm
     ```
     (where <xxxx> is a series of numbers representing the version and build numbers)
   - If you are installing from the tar installation archive, unpack the archive.
     ```
     tar zxf VMware-console-<xxxx>.tar.gz
     ```
     (where <xxxx> is a series of numbers representing the version and build numbers)

     The archive unpacks to `vmware-console-distrib`.

     Run the installer.
     ```
     cd vmware-console-distrib
     ./vmware-install.pl
     ```

     Accept the EULA and answer the questions specifying default directories.

     If the `Do you accept ...` prompt doesn't appear, press `Q` to continue.

     At the prompt `What port do you want the remote console to use to connect to server. [902]` If you specified a different port number when you installed the server software, enter that port number here. Otherwise, keep the default of 902.

Installing the VMware Scripting APIs

VMware GSX Server supports the VMware Scripting APIs, which include the VmPerl API and the VmCOM API. You can use the VMware Scripting APIs to manage the GSX Server host and virtual machines locally and remotely.

For more information, go to *www.vmware.com/support/developer*.

Installing the VmPerl and VmCOM Scripting APIs on a Windows Host

On a Windows machine, either the server host or remote computer, you can use either the VmPerl API or the VmCOM API. Both scripting APIs are installed automatically on the GSX Server for Windows host from the master installer if you chose a complete installation. In addition, you can make the APIs available for download by customizing the download menu on the Login page of the VMware Management Interface. For more information, see Downloading Remote Management Packages on page 175.

You have a choice of installing either the VmCOM or the VmPerl Scripting API, or both.

1. Choose **Start** > **Run** and browse to the directory where you saved the downloaded installer file (the name is similar to `VMware-VmPerlAPI-<xxxx>.exe` or `VMware-VmCOMAPI-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers).
2. The installer starts. Click **Next**.
3. Acknowledge the end user license agreement (EULA). Select **Yes, I accept the terms in the license agreement**, then click **Next**.
4. Choose the directory in which to install the scripting API. To install it in a directory other than the default, click **Change** and browse to your directory of choice. If the directory does not exist, the installer creates it for you. Click **Next**.

   Note: Windows and the Microsoft Installer limit the path length to 255 characters for a path to a folder on a local drive and 240 characters for a path to a folder on a mapped or shared drive. If the path to the scripting API program folder exceeds this limit, an error message appears. You must select or enter a shorter path.
5. Click **Install**. The installer begins copying files to your machine.
6. Click **Finish**. The VMware Scripting API is installed.

If you install the VmCOM API, two folders named MiniMUI and SampleScripts are created in the same directory as the VmCOM Scripting API. The MiniMUI folder

contains a sample Microsoft Visual Basic 6 project that uses VmCOM. The SampleScripts folder contains VBScript and JScript samples using the VmCOM Scripting API.

If you install the VmPerl API, a SampleScripts folder is created in the same directory as the VmCOM Scripting API. The SampleScripts folder contains sample scripts using the VmPerl Scripting API.

Installing the VmPerl Scripting API on a Linux Host

On a Linux machine, either the server host or remote computer, you can use only the VmPerl Scripting API. The VmCOM API cannot be installed on a Linux host; although the VmCOM API installed on a Windows remote workstation can communicate with a Linux host. You can make the VmPerl API tar archive available for download by customizing the download menu on the Login page of the VMware Management Interface. See Downloading Remote Management Packages on page 175.

1. Download the VmPerl API package from the VMware Management Interface Login page to the machine on which you want to run the VMware Scripting API.
2. Untar the package.
   `tar zxf VMware-VmPerlAPI-<xxxx>.tar.gz`
   (where `<xxxx>` is a series of numbers representing the version and build numbers)
3. Change to the installation directory.
   `cd vmware-api-distrib`
4. Run the installation program.
   `./vmware-install.pl`
5. Press Enter to read the end user license agreement (EULA). You may page through it by pressing the spacebar. If the `Do you accept?` prompt doesn't appear, press `Q` to get to the next prompt. Accept the EULA.
6. Specify the directory where you want to install the VmPerl Scripting API executable files. The default is the directory where Perl is installed on your host, typically `/usr/bin`.
7. Specify the directory where you want to install the VmPerl Scripting API library files. The default is `/usr/lib/vmware-api`.

   This directory includes the sample scripts for the VmPerl API. The SampleScripts directory contains example scripts that demonstrate use of the VmPerl API. You may customize these scripts for your particular organization.
8. Specify the directory where you want to install the VmPerl Scripting API documentation files. These files consist of the README, end user license agreement and copyright information. The default is `/usr/share/doc/vmware-api`.

Uninstalling VMware GSX Server

The following sections describe how to remove the GSX Server components from your system. Follow the steps for your host operating system.

Uninstalling GSX Server on a Windows Host

To uninstall GSX Server, complete the following steps. This removes all the components you installed with the GSX Server master installer, including the server software, the VMware Management Interface, the VMware Remote Console and the VMware Scripting APIs.

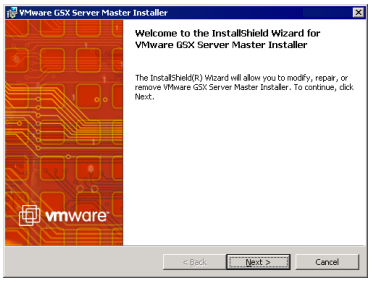
If you chose the custom installation path, any components you installed at that time are removed when you use the master installer to uninstall GSX Server.

1. On a Windows Server 2003 host, choose **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**. Select the **VMware GSX Server Master Installer** and click **Change**.

   On a Windows 2000 host, choose **Start** > **Settings** > **Control Panel** > **Add/ Remove Programs**. Select the **VMware GSX Server Master Installer** and click **Change**.

   On a Windows NT host, run the **VMware GSX Server Master Installer** from its location on your host.

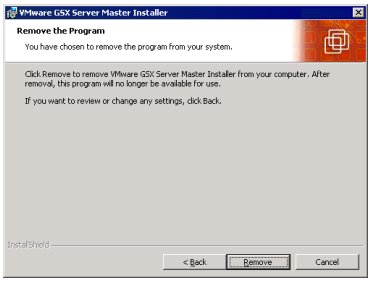
2. After the master installer launches, click **Next**.


VMware GSX Server Master Installer
Welcome to the InstallShield Wizard for VMware GSX Server Master Installer
The InstallShield(R) Wizard will allow you to modify, repair, or remove VMware GSX Server Master Installer. To continue, click Next.
vmware
< Back
Next >
Cancel

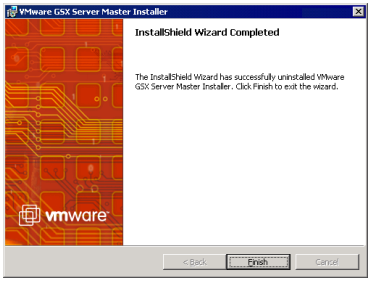
3. Select **Remove**, then click **Next**.

VMware GSX Server Master Installer
Program Maintenance
Modify, repair, or remove the program.
Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
Repair
Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.
Remove
Remove all GSX Server components from your computer.
InstallShield
< Back
Next >
Cancel

4. When you are ready to begin removing GSX Server, click **Remove**.


VMware GSX Server Master Installer
Remove the Program
You have chosen to remove the program from your system.
Click Remove to remove VMware GSX Server Master Installer from your computer. After removal, this program will no longer be available for use.
If you want to review or change any settings, click Back.
InstallShield
< Back
Remove
Cancel

5. During the uninstallation, you are asked whether you want to remove your VMware licenses from the registry. VMware strongly recommends you keep your licenses, in case you reinstall or upgrade your software. To keep the licenses in the registry, click **No**. The uninstallation continues.
6. After all the components (including the server software, the management interface, the remote console and the scripting APIs) are removed, click **Finish**.


VMware GSX Server Master Installer
InstallShield Wizard Completed
The InstallShield Wizard has successfully uninstalled VMware GSX Server Master Installer. Click Finish to exit the wizard.
vmware
< Back
Finish
Cancel

7. You are prompted to reboot your system. Click **Yes** to reboot.

Uninstalling GSX Server on a Linux Host

If you used the RPM installer to install GSX Server, remove the software from your system by running

```
rpm -e VMware-gsx
```

If you used the tar installer to install GSX Server, remove the software from your system by running

```
vmware-uninstall.pl
```

To uninstall the VMware Management Interface components, type

```
/home/vmware/mui/bin/vmware-uninstall-mui.pl
```

To uninstall a Linux remote console that was installed from an RPM package, type the following

```
rpm -e VMware-console
```

To uninstall a Linux remote console that was installed from a tar package, run the program

```
/usr/bin/vmware-uninstall-console.pl
```

To uninstall the VmPerl API, type the following

```
/usr/bin/vmware-uninstall-api.pl
```

3

Upgrading VMware GSX Server

Upgrading VMware GSX Server

The following sections describe how to upgrade VMware GSX Server on your Linux or Windows host system and how to use virtual machines created under earlier versions of GSX Server with the current version:

- Preparing for the Upgrade on page 73
- Upgrading on a Windows Host on page 75
- Upgrading on a Linux Host on page 78
- Upgrading the Virtual Hardware in Older Windows Guest Operating Systems on page 80

Preparing for the Upgrade

Before You Install GSX Server

There are a few steps you should take — before you remove an already installed version of GSX Server and install the new version of GSX Server — to ensure the best possible upgrade experience.

Resume and Shut Down Suspended Virtual Machines

If you plan to use virtual machines created under an earlier version of GSX Server, be sure they have been shut down completely before you remove the release you used to create them.

If the virtual machine is suspended, resume it in the earlier release, shut down the guest operating system, then power off the virtual machine.

Note: If you attempt to resume a virtual machine that was suspended under a different VMware product or a different version of GSX Server, a dialog box gives you the choice of discarding or keeping the file that stores the suspended state. To recover the suspended state, you must click **Keep**, then resume the virtual machine under the correct VMware product. If you click **Discard**, you can power on normally, but the suspended state is lost.

Commit or Discard Changes to Disks in Undoable Mode

If you plan to use existing virtual machines that have disks in undoable mode, commit or discard any changes to the virtual disks before you remove the release you used to create them.

Resume or power on the virtual machine in the earlier release, shut down the guest operating system, power off the virtual machine and either commit or discard changes to the disk in undoable mode when prompted.

Remove VMware GSX Server or VMware Workstation

If you have GSX Server installed on your host system, you must remove it before you install the new version. Also, see When You Remove an Existing Version and Install the New Version on page 74.

If you have VMware Workstation installed on your host system, you must remove it before you install GSX Server. See the VMware Workstation product documentation for information on how to remove Workstation.

Back Up Virtual Machines

As a precaution, back up all the files in your virtual machine directories — including the `.vmdk` or `.dsk`, `.cfg` or `.vmx` and `nvram` files — for any existing virtual machines you plan to migrate to the new version of GSX Server.

Virtual machines updated for full compatibility with GSX Server 2 cannot be used under GSX Server 1.

When You Remove an Existing Version and Install the New Version

There is a key precaution you should take when you remove an existing installation of GSX Server and install the new version.

Leave the Existing License in Place

The installation steps for your host may require that you run an uninstaller to remove a previous version of GSX Server from your machine.

On a Windows host, the uninstaller offers to remove licenses from your registry. If you think you may want to use the previous version of GSX Server again, do not remove the licenses. You can safely keep licenses for multiple VMware products on the computer at the same time.

On a Linux host, the license remains in place. You do not need to take any special action. You may safely leave the license where it is.

Upgrading on a Windows Host

Upgrading to the Latest Version

The Upgrade Process

Upgrading your GSX Server software is a four-step process.

1. Uninstall the current version. If you are uninstalling an earlier version of GSX Server 2, see Uninstalling GSX Server on a Windows Host on page 68. If you are uninstalling GSX Server 1, see Removing Version 1 below.
2. Reboot your computer.
3. Install the latest version. See Installing VMware GSX Server on a Windows Host on page 40.
4. Reboot your computer.

If you have virtual machines you created under GSX Server 1 you want to keep using with GSX Server 2, see Using Virtual Machines Created with Version 1 under the New Version on page 75.

Upgrading from GSX Server 1

Removing Version 1

To uninstall GSX Server 1, use Add/Remove Programs in the Windows Control Panel. Be sure to uninstall GSX Server, the VMware Management Interface and the VMware Remote Console.

After you remove the three packages, reboot your host and follow the instructions in Installing VMware GSX Server on a Windows Host on page 40.

Note: If you have VMware Workstation installed on your host system, you must remove it before you install GSX Server. See the VMware Workstation product documentation for information on how to remove Workstation.

Using Virtual Machines Created with Version 1 under the New Version

There are, broadly speaking, three approaches you can take to setting up virtual machines under GSX Server 2. Choose the approach or combination of approaches that best suit your needs.

- Create everything new from the start. Use the New Virtual Machine Wizard to set up a new virtual machine and install a guest operating system in the virtual machine as described in Creating New Virtual Machines on page 83. If you set up

your virtual machines in this way, you will be using the latest technology and will enjoy the best possible virtual machine performance.

- Use an existing configuration file (`.vmx`) and virtual disk (`.dsk` if you do not convert to new filenames when you install GSX Server or `.vmdk` if you do convert).

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 113. Do not remove the older version of VMware Tools before installing the new version.

  A virtual machine set up in this way should run without problems. However, you will not have USB ports.

  Note: On Windows hosts, GSX Server 2 offers to convert virtual disk `.dsk` filenames to use the new `.vmdk` extension at the time you install GSX Server. The `.vmdk` extension can be used for virtual disks under any VMware product. GSX Server automatically updates references to the virtual disk files in configuration files on the host computer. If you are using the same virtual disk file from any other computer, you need to update the configuration files with the new filename. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 376.

- Use an existing virtual machine and upgrade the virtual hardware. This gives you access to new features, but the process is one-way — you cannot reverse it.

  Start by using an existing configuration file (`.vmx`) and virtual disk (`.dsk` if you do not convert to new filenames when you install GSX Server or `.vmdk` if you do convert).

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 113. Do not remove the older version of VMware Tools before installing the new version.

  Upgrade the virtual hardware so you can use USB devices in your virtual machine. Power off the virtual machine. On the **Settings** menu in the local console window, choose **Upgrade Virtual Hardware**. A dialog box appears, warning that the upgrade process cannot be reversed. Click **Yes** to continue, then follow the directions.

  Note: If you are upgrading the virtual hardware for Windows Me, Windows 98 or Windows 95 guest operating system, there are additional steps. See Upgrading the Virtual Hardware in Older Windows Guest Operating Systems on page 80.

Virtual Hardware Upgrade Is Irreversible

- The process of upgrading the virtual hardware is irreversible and makes the disks attached to this virtual machine incompatible with VMware GSX Server 1. You should make backup copies of your virtual disks before starting the upgrade.

Note: On Windows hosts, GSX Server 2 offers to convert virtual disk `.dsk` filenames to use the new `.vmdk` extension at the time you install GSX Server. The `.vmdk` extension can be used for virtual disks under any VMware product. GSX Server automatically updates references to the virtual disk files in configuration files on the host computer. If you are using the same virtual disk file from any other computer, you need to update the configuration files with the new filename. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 376.

Upgrading on a Linux Host

Removing the Existing Version

If you used the tar installer to install your current version of GSX Server, and you plan to use the tar installer for the new version, the only special step you need to take is to make sure the directory to which you plan to untar the tar archive does not contain any files from a previous GSX Server tar installation. You do not need to uninstall the older version. Just follow the installation instructions under Installing VMware GSX Server on a Linux Host on page 50.

If you used the RPM installer to install your current version of GSX Server, you need to uninstall the software before you upgrade to the new version. See Uninstalling GSX Server on a Linux Host on page 70.

Using Virtual Machines Created with Version 1 under the New Version

There are, broadly speaking, three approaches you can take to setting up virtual machines under GSX Server 2. Choose the approach or combination of approaches that best suit your needs.

- Create everything new from the start. Use the Configuration Wizard to set up a new virtual machine and install a guest operating system in the virtual machine as described in Creating New Virtual Machines on page 83. If you set up your virtual machines in this way, you will be using the latest technology and will enjoy the best possible virtual machine performance.
- Use an existing configuration file (`.cfg`) and virtual disk (`.dsk` if you do not convert to new filenames when you install GSX Server or `.vmdk` if you do convert).

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 113. You should not remove the older version of VMware Tools before installing the new version.

  A virtual machine set up in this way should run without problems. However, you will not have the benefits of certain new features. You will not have USB ports. You will not have the new BIOS, which makes it easier to use one of the operating systems on a dual-boot host machine as a guest operating system in a virtual machine. Also, you will not have the new unified virtual video hardware, which helps simplify the installation of VMware Tools.

- Use an existing virtual machine and upgrade the virtual hardware. This gives you access to new features, but the process is one-way — you cannot reverse it.

  Start by using an existing configuration file (`.cfg`) and virtual disk (`.dsk` if you do not convert to new filenames when you install GSX Server or `.vmdk` if you do convert).

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 113. You should not remove the older version of VMware Tools before installing the new version.

  Upgrade the virtual hardware so you can use USB devices in your virtual machine. Power off the virtual machine. On the **Settings** menu in the local console window, choose **Upgrade Virtual Hardware**. A dialog box appears, warning that the upgrade process cannot be reversed. Click **Yes** to continue, then follow the directions.

  Note: If you are upgrading the virtual hardware for Windows Me, Windows 98 or Windows 95 guest operating system, there are additional steps. See Upgrading the Virtual Hardware in Older Windows Guest Operating Systems on page 80.

Virtual Hardware Upgrade Is Irreversible

- The process of upgrading the virtual hardware is irreversible and makes the disks attached to this virtual machine incompatible with VMware GSX Server 1. You should make backup copies of your virtual disks before starting the upgrade.

Upgrading the Virtual Hardware in Older Windows Guest Operating Systems

If you are using a Windows Me, Windows 98 or Windows 95 virtual machine created under GSX Server 1 and choose to upgrade the virtual hardware, you need to take several steps to be sure the new virtual hardware is recognized properly by the guest operating system. With other guest operating systems, these special steps are not needed.

Before you upgrade the virtual hardware, make sure you have installed the latest version of VMware Tools, including the SVGA driver, then power off your virtual machine.

Follow the steps listed under the name of your guest operating system.

Windows Me Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: "This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
5. Several Plug and Play messages appear. You can safely ignore them.
6. Log on to Windows Me. More Plug and Play messages are displayed. One refers to the VMware SVGA driver.

   Click **Yes** to restart your computer.
7. Log on to Windows Me. The SVGA driver is not working properly.
8. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

   Manually remove the two SVGA drivers.
9. Restart Windows Me.

   A VMware SVGA II adapter is detected and Windows installs it.

   Windows notifies you to restart your computer.

   Click **Yes**.
10. The SVGA driver should be working correctly.

Windows 98 Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: "This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
5. Log on to Windows 98. You see a number of Plug and Play messages. You may need to insert your Windows 98 installation CD.
6. A blue screen appears. Press any key to dismiss the blue screen.
7. Click **Reset** to restart the virtual machine (because it is not responding).
8. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."

   Again, you see a number of Plug and Play messages.

   Windows notifies you to restart Windows.

   Click **Yes**.
9. Log on to Windows 98. The SVGA driver is not working properly.
10. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

    Manually remove the two conflicting SVGA drivers.
11. Restart Windows 98.

    A VMware SVGA II adapter is detected and Windows installs it.
12. Restart Windows 98.
13. The SVGA driver should be working correctly.

Windows 95 Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: "This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."

5. Log on to Windows 95. You see a number of Plug and Play messages. Click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.

   The SVGA driver is not working properly.

6. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

   Manually remove the SVGA driver.

7. Restart Windows 95.
8. Again, you see a number of Plug and Play messages. Click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
9. A VMware SVGA II adapter is detected and Windows installs it.
10. Restart Windows 95.
11. Once again, you see a number of Plug and Play messages. Again, click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
12. The SVGA driver should be working correctly.

Check Guest Operating System Selection

Some operating systems, such as Windows Server 2003 and Windows 2000, have multiple versions. Verify your guest operating system is set to the specific version of the operating system installed in the virtual machine. Check the setting in the Configuration Editor (**Settings** > **Configuration Editor** > **Options**).

4

Creating New Virtual Machines

Creating a New Virtual Machine

The following sections describe how to create a new virtual machine on Windows and Linux hosts using a wizard in the GSX Server local console.

- Setting Up a New Virtual Machine on a Windows Host on page 85
  - What's in a Virtual Machine on a Windows Host? on page 85
  - Simple Steps to a New Virtual Machine on a Windows Host on page 86
- Setting Up a New Virtual Machine on a Linux Host on page 94
  - What's in a Virtual Machine on a Linux Host? on page 94
  - Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host on page 96
  - Simple Steps to a New Virtual Machine on a Linux Host on page 97
- Installing a Guest Operating System on page 107
  - Example: Installing Windows 2000 as a Guest Operating System on page 107

Note: If you are not on the host system, you can create virtual machines remotely from the VMware Management Interface. For more information, see Creating a New Virtual Machine from the Management Interface on page 177.

Setting Up a New Virtual Machine on a Windows Host

The New Virtual Machine Wizard guides you through the key steps for setting up a new virtual machine, helping you set various options and parameters. You can then use the Configuration Editor (**Settings** > **Configuration Editor**) if you need to make any changes to your virtual machine's setup.

A new virtual machine is like a physical computer with a blank hard disk. Before you can use it, you need to format the virtual disk and install a guest operating system. The operating system's installation program may handle the formatting step for you.

What's in a Virtual Machine on a Windows Host?

The virtual machine typically is stored on the host computer in a set of files, all of which are in a folder set aside for that particular virtual machine. In these examples, `<vmname>` is the name of your virtual machine. The key files are:

- `<vmname>.vmx` — the configuration file, which stores settings chosen in the New Virtual Machine Wizard or Configuration Editor.
- `<vmname>.vmx.bak` — the backup configuration file, which you can use if your original configuration file becomes corrupted or lost.
- `nvram` — the file that stores the state of the virtual machine's BIOS.
- `<vmname>.vmdk` — the virtual disk file, which stores the contents of the virtual machine's hard disk drive. A virtual disk comprises one or more `.vmdk` files. The larger the size of the virtual disk, the more `.vmdk` files. As data is added to a virtual disk, the `.vmdk` files grow in size, to a maximum of 2GB each. Almost all of a `.vmdk` file's content is the virtual machine's data, with a small portion allotted to virtual machine overhead. If the virtual disk is 2GB or larger, GSX Server creates multiple `.vmdk` files.

  If the virtual machine contains plain disks, a type of virtual disk where all the space for the disk is allocated when you create it, there is no `.vmdk` file. Instead, a `.pln` file stores information about the virtual disk, and the actual virtual machine data is stored in a series of `.dat` files.

  If the virtual machine is connected directly to a physical disk, rather than using a virtual disk, there is no `.vmdk` file. Instead, a `.raw` file stores information about the partitions the virtual machine is allowed to access.

  Note: Earlier VMware products used the extension `.dsk` for virtual disk files.

- `vmware.log` — the file that keeps a log of key GSX Server activity. This can be useful in troubleshooting if you encounter problems. This file is stored in the folder that holds the configuration (`.vmx`) file of the virtual machine.
- `<vmname>.vmdk.REDO` — the redo-log file, created automatically when a virtual machine is used in undoable or nonpersistent mode. This file stores changes made to the virtual disk while the virtual machine is running. The redo-log file for a virtual disk in nonpersistent mode is stored in the `temp` directory of the user who created the virtual machine.
- `<vmname>.vmss` — the suspended state file, which stores the state of a suspended virtual machine.

  Note: Earlier VMware products used the extension `.std` for suspended state files.

There may be other files as well, some of which are present only while a virtual machine is running.

Permissions and Running Virtual Machines

As you create virtual machines, be aware that in order for other users to run a virtual machine you create, those users must have the same level of permissions as your user account. For example, if you are an administrator, only users with administrator privileges can see and connect to virtual machines you created. However, a user with administrator privileges can see and connect to virtual machines created by a non-administrator user.

Simple Steps to a New Virtual Machine on a Windows Host

By default, the new virtual machine uses an IDE disk in persistent mode for Windows 95, Windows 98, Windows Me, Windows XP and Windows Server 2003 guests. The default for other guest operating systems is a SCSI disk in persistent mode.

Follow these steps to create a virtual machine using a virtual disk.

1. Open the local console. Choose **Start** > **Programs** > **VMware** > **VMware GSX Server**.

   (Or, double-click the VMware GSX Server icon on your desktop.)

2. If this is the first time you have launched GSX Server, you are prompted to enter your 20-character serial number. This number is included in the email message

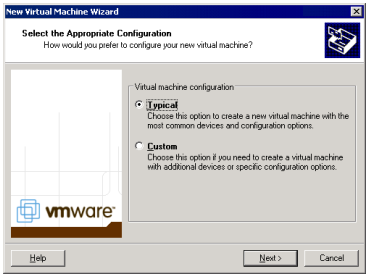
you received from VMware or the reseller from whom you purchased GSX Server. Enter your serial number and click **OK**.

The serial number you enter is saved and GSX Server does not ask you for it again. For your convenience, GSX Server automatically sends the serial number to the VMware Web site when you use certain Web links built into the product (for example, **Help** > **VMware software on the Web** > **Register Now!** and **Help** > **VMware software on the Web** > **Request Support**). This allows us to direct you to the correct Web page for registration and support for your product.

Note: If you are upgrading from an earlier version with the same major release number (for example, from 2.0 to 2.5), you do not need to enter a serial number.

3. Start the New Virtual Machine Wizard. Click the New Virtual Machine icon.

4. The New Virtual Machine Wizard presents you with a series of screens that you navigate using the **Next** and **Back** buttons at the bottom of each screen. At each screen, follow the instructions, then click **Next** to proceed to the next screen.
5. Select the method you want to use for configuring your virtual machine.


New Virtual Machine Wizard
Select the Appropriate Configuration
How would you prefer to configure your new virtual machine?
Virtual machine configuration
Typical
Choose this option to create a new virtual machine with the most common devices and configuration options.
Custom
Choose this option if you need to create a virtual machine with additional devices or specific configuration options.
vmware
Help
Next >
Cancel

If you select **Typical**, the wizard prompts you to specify or accept defaults for

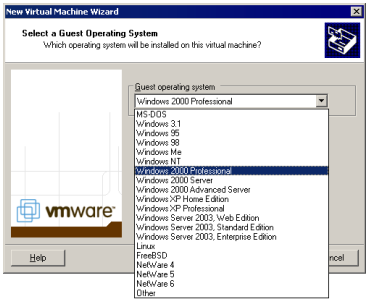
- The guest operating system.
- The virtual machine name and the location of the virtual machine's files.
- The network connection type.

Select **Custom** if you want to

- Make a virtual disk larger or smaller than 4GB.
- Store your virtual disk's files in a particular location.

- Use an IDE virtual disk for a guest operating system that would otherwise have a SCSI virtual disk created by default or vice versa.
- Use an existing virtual disk.
- Create a plain disk for clustering or better performance.
- Use a physical disk rather than a virtual disk (for expert users).
- Change the amount of memory allocated.

6. Select a guest operating system.

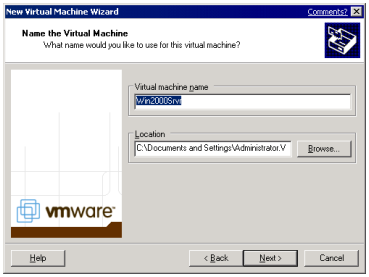


This screen asks which operating system you plan to install in the virtual machine. The New Virtual Machine Wizard uses this information to select appropriate default values, such as the amount of disk space needed. The wizard also uses this information when naming associated virtual machine files.

If the operating system you are using is not listed, select **Other**.

You can find detailed installation notes for guest operating systems in Installing Guest Operating Systems on page 251.

7. Select a name and folder for the virtual machine.

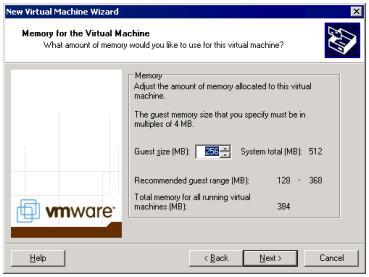


The name specified here appears in the Virtual Machine Name list in the local console, the VMware Management Interface and the Connect to VMware Virtual Machine dialog box that appears when you connect to a virtual machine with the VMware Remote Console. It is also used as the name of the folder where the files associated with this virtual machine are stored.

Each virtual machine should have its own folder. All associated files, such as the configuration file and the disk file, are placed in this folder. On Windows 2000 and Windows Server 2003 hosts, the default folder is `C:\Documents and Settings\<username>\My Documents\My Virtual Machines\<guestOS>`, where `<guestOS>` is an abbreviation of the guest operating system you selected in the previous panel. On a Windows NT host, the default folder is `C:\WINNT\Profiles\<username>\Personal\My Virtual Machines\<guestOS>`. You can change the default in the local console; choose **Settings** > **Preferences**, then click the **Workspace** tab. Click **Browse** to select a new path.

Virtual machine performance may be slower if your virtual hard disk is on a network drive. For best performance, be sure the virtual machine's folder is on a local drive. However, if other users need to access this virtual machine, you should consider placing the virtual machine files in a location that is accessible to them. For more information, see Sharing Virtual Machines with Other Users on page 250.

8. Specify the amount of memory for the virtual machine.


New Virtual Machine Wizard
Memory for the Virtual Machine
What amount of memory would you like to use for this virtual machine?
Memory
Adjust the amount of memory allocated to this virtual machine.
The guest memory size that you specify must be in multiples of 4 MB.
Guest size (MB):
System total (MB): 512
Recommended guest range (MB): 128 - 368
Total memory for all running virtual machines (MB): 384
vmware
Help
< Back
Next >
Cancel

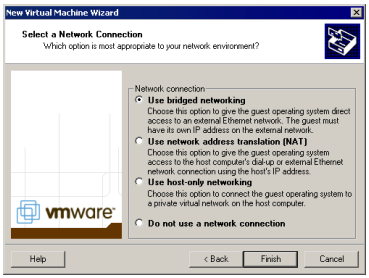
The New Virtual Machine Wizard provides a default value based on your guest operating system, along with the recommended range and the total amount of memory reserved for all running virtual machines.

To change the amount of memory to be allocated to the virtual machine, click the arrows next to the **Guest size (MB)** field or type a new value in the field.

If you selected a **Typical** installation, the wizard automatically allocates the default value for memory and this panel does not appear.

For more information about memory, see Understanding Memory on page 529.

9. Configure the networking capabilities of the virtual machine.


New Virtual Machine Wizard
Select a Network Connection
Which option is most appropriate to your network environment?
Network connection
Use bridged networking
Choose this option to give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
Use network address translation (NAT)
Choose this option to give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
Use host-only networking
Choose this option to connect the guest operating system to a private virtual network on the host computer.
Do not use a network connection
vmware
Help
< Back
Finish
Cancel

If your host computer is on a network and you have a separate IP address for your virtual machine (or can get one automatically from a DHCP server), select **Use bridged networking**.

If you do not have a separate IP address for your virtual machine but you want to be able to connect to the Internet, select **Use network address translation (NAT)**. NAT is useful if you have a wireless NIC on your host (as bridged networking is not supported on wireless NICs) and allows for the sharing of files between the virtual machine and the host operating system.

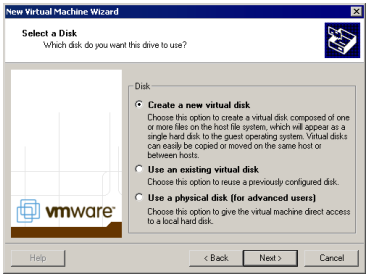
To enable your virtual machine to use a virtual network limited to the host and the virtual machines running on the host, select **Use host-only networking**.

For more details about GSX Server networking options, see Networking on page 403.

10. If you selected **Typical** as your configuration path, click **Finish** and the wizard sets up the files needed for your virtual machine.

    If you selected **Custom** as your configuration path, continue with the steps for configuring a disk for your virtual machine.

11. Select the disk type.


New Virtual Machine Wizard
Select a Disk
Which disk do you want this drive to use?
Disk
Create a new virtual disk
Choose this option to create a virtual disk composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk.
vmware
Help
< Back
Next >
Cancel

Select **Create a new virtual disk**.

Virtual disks are the best choice for most virtual machines. They are quick and easy to set up and can be moved to new locations on the same host computer or to different host computers. Virtual disks start as small files on the host computer's hard drive, then expand as needed — up to the size you specify in the next step.

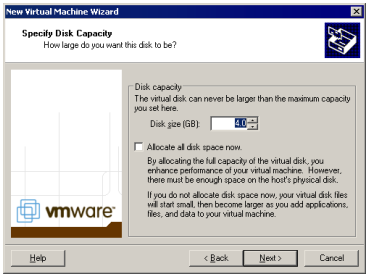
To use an existing virtual disk, select **Use an existing virtual disk**.

To install your guest operating system directly on an existing IDE disk partition, read the reference note Installing an Operating System onto a Raw Partition from a Virtual Machine on page 396.

To install the guest operating system on a raw IDE disk, select **Use a physical disk**. To use a raw SCSI disk, add it to the virtual machine later with the Configuration Editor. Booting from a raw SCSI disk is not supported.

Caution: Raw disk configurations are recommended only for expert users.

12. Specify the size of the virtual disk.


New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
Disk capacity
The virtual disk can never be larger than the maximum capacity you set here.
Disk size (GB):
40
Allocate all disk space now.
By allocating the full capacity of the virtual disk, you enhance performance of your virtual machine. However, there must be enough space on the host's physical disk.
If you do not allocate disk space now, your virtual disk files will start small, then become larger as you add applications, files, and data to your virtual machine.
vmware
Help
< Back
Next >
Cancel

Enter the size of the virtual disk that you wish to create. Use the default of 4GB or change the setting. The maximum size is 128GB for an IDE virtual disk or 256GB

Make the Virtual Disk Big Enough

- The virtual disk should be large enough to hold the guest operating system and all of the software that you intend to install, with room for data and growth.
- You cannot change the virtual disk's maximum capacity later.
- You can install additional virtual disks using the Configuration Editor.
- For example, you need about 750MB of actual free space on the file system containing the virtual disk to install Windows 2000 and popular applications such as Microsoft Office inside the virtual machine. You can set up a single virtual disk to hold these files. Or you can split them up — installing the operating system on the first virtual disk and using a second virtual disk for applications or data files.

for a SCSI virtual disk. When you specify the size of the virtual disk, that amount of disk space is not immediately occupied by the virtual disk files. The virtual disk files grow as needed when applications and files are added to them, until the virtual disk reaches the maximum capacity you specify here.

Note: If this setting is larger than the capacity of the host machine's hard disk, a warning message appears. You can ignore this message for now, as you can move this virtual machine to a drive that can hold it at a later time.

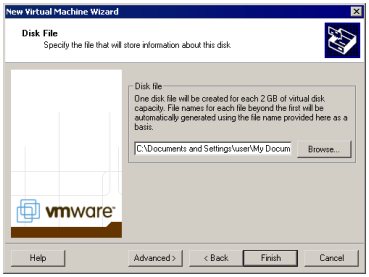
If you want to improve virtual machine performance, you can choose to allocate all the full capacity of the virtual disk on the host at the time you create the disk. This type of virtual disk is called a plain disk. Be aware of how much available space you have on your host or wherever you choose to create the disk. Also note that plain disks take longer to create.

To allocate the disk space upon creation, check **Allocate all disk space now.** The virtual disk files do not have a `.vmdk` extension; instead, a file called `<virtual machine>.pln` is created that contains information about the virtual disk. The data for the virtual disk is stored in a set of files called `<virtual machine><n>.dat`, with one `.dat` file created for each 2GB of disk capacity.

Note: If this setting is larger than the capacity of the host machine's hard disk, a warning message appears, and specifies how much space you have on the host. If the disk will exceed the available space on the host, you must make the virtual disk smaller.

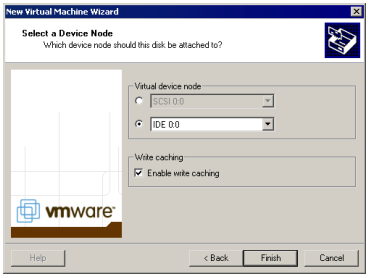
This type of virtual disk is useful for clustering virtual machines. For more information about clustering, see High-Availability Configurations with GSX Server on page 539.

13. Specify the location of the virtual disk's files.


New Virtual Machine Wizard
Disk File
Specify the file that will store information about this disk
Disk file
One disk file will be created for each 2 GB of virtual disk capacity. File names for each file beyond the first will be automatically generated using the file name provided here as a basis.
C:\Documents and Settings\user\My Docum
Browse...
vmware
Help
Advanced >
< Back
Finish
Cancel

If a SCSI virtual disk is selected and you want to use a virtual IDE disk instead, or if you want to specify which device node should be used by your SCSI or IDE virtual disk, click **Advanced**.

14. Click **Finish** and the wizard sets up the files needed for your virtual machine.



Setting Up a New Virtual Machine on a Linux Host

The Configuration Wizard guides you through the key steps for setting up a new virtual machine, helping you set various options and parameters. You can then use the Configuration Editor (**Settings** > **Configuration Editor**) if you need to make any changes to your virtual machine's setup.

A new virtual machine is like a physical computer with a blank hard disk. Before you can use it, you need to format the virtual disk and install a guest operating system. The operating system's installation program may handle the formatting step for you.

Caution: If you are creating a virtual machine on a SuSE Linux 8.1, 8.2 or SLES 8 host, please see Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host on page 96 before you create any virtual machines.

What's in a Virtual Machine on a Linux Host?

The virtual machine typically is stored on the host computer in a set of files, all of which are in a directory set aside for that particular virtual machine. In these examples, `<vmname>` is the name of your virtual machine. The key files are:

- `<vmname>.cfg` — the configuration file, which stores settings chosen in the Configuration Wizard or Configuration Editor.
- `nvram` — the file that stores the state of the virtual machine's BIOS.
- `<vmname>.vmdk` — the virtual disk file, which stores the contents of the virtual machine's hard disk drive. If the virtual disk is larger than 2GB, GSX Server creates multiple `.vmdk` files, one for each 2GB of disk space. If the virtual machine is connected directly to a physical disk, rather than using a virtual disk, there is no `.vmdk` file. Instead, a `.raw` file stores information about the partitions the virtual machine is allowed to access.

  Note: Earlier VMware products used the extension `.dsk` for virtual disk files.

  If the virtual machine contains plain disks, a type of virtual disk where all the space for the disk is allocated when you create it, there is no `.vmdk` file. Instead, a `.pln` file stores information about the virtual disk, and the actual virtual machine data is stored in a series of `.dat` files.
- `<vmname>.log` or `vmware.log` — the file that keeps a log of key GSX Server activity. This can be useful in troubleshooting if you encounter problems.

This file is stored in the directory that holds the configuration (`.cfg`) file of the virtual machine.

- `<vmname>.vmdk.REDO` — the redo-log file, created automatically when a virtual machine is used in undoable or nonpersistent mode. This file stores changes made to the virtual disk while the virtual machine is running. The redo-log file for a virtual disk in nonpersistent mode is stored in the `temp` directory of the user who created the virtual machine.
- `<vmname>.vmss` — the suspended state file, which stores the state of a suspended virtual machine.

  Note: Earlier VMware products used the extension `.std` for suspended state files.

There may be other files as well, some of which are present only while a virtual machine is running.

By default, the new virtual machine uses an IDE disk in persistent mode for Windows 95, Windows 98, Windows Me, Windows XP and Windows Server 2003 guests. The default for other guest operating systems is a SCSI disk in persistent mode.

Before you begin configuring your virtual machine, check the following notes and make any necessary adjustments to the configuration of your host operating system.

- The real time clock function must be compiled into your Linux kernel
- GSX Server for Linux requires that the parallel port "PC-style hardware" option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module (that is, it must be set to `"m"` when the kernel is compiled).

Permissions and Running Virtual Machines

When you create a virtual machine with GSX Server, its configuration file is registered with the following default permissions, based on the user accessing it:

- **Read**, **execute** and **write** — for the user who created the virtual machine (the owner)
- **Read** and **execute** — for the owner's group
- **Read** — for users other than the owner or a member of the owner's group

You can change these permissions as needed, for example, if users in different groups need to access a particular virtual machine.

Before You Create Virtual Machines on a SuSE Linux 8.1, 8.2 or SLES 8 Host

If you try to power on a virtual machine on a SuSE Linux 8.1, 8.2 or SLES 8 host, a segmentation fault error occurs. In order to run virtual machines on a SuSE Linux 8.1, 8.2 or SLES 8 host, you must boot the host with the `apic` parameter. You can enter this parameter into the boot loader file to avoid having to specify it every time you boot the SuSE Linux host. For more information and instructions on how to modify the boot loader file, go to *sdb.suse.com/en/sdb/html/fhassel_vmware_segfault81.html*.

SuSE also cautions that "in some few cases (in connection with certain hardware), the use of the kernel parameter 'apic' may result in an unstable Linux system. In these cases you will not be able to use the application VMware with the SuSE Linux 8.1 kernel."

Simple Steps to a New Virtual Machine on a Linux Host

Follow these steps to create a virtual machine using a virtual disk.

1. In a terminal window, open a local console.

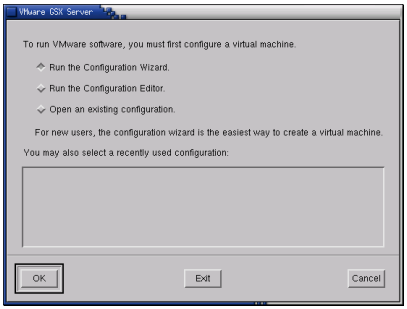
   ```
   vmware -G
   ```

2. If this is the first time you have launched GSX Server, a dialog box asks if you want to rename existing virtual disks using the new `.vmdk` extension. Click **OK** to search all local drives on the host computer and make this change.

   The converter also renames the files that store the state of a suspended virtual machine, if it finds them. It changes the old `.std` file extension to `.vmss`. However, it is best to resume and shut down all suspended virtual machines before you upgrade to GSX Server 2.

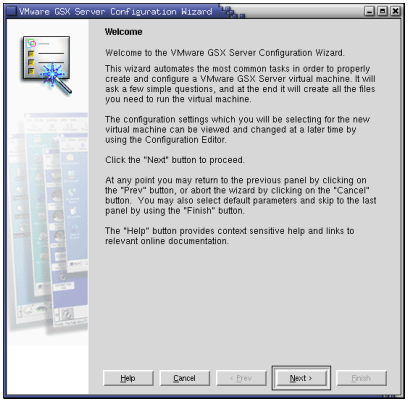
   Besides renaming files, the converter updates the corresponding virtual machine configuration files so they identify the virtual disks using the new filenames.

3. Start the Configuration Wizard. The default selection is **Run the Configuration Wizard**. To start the Configuration Wizard, click **OK**. You can also start the Configuration Wizard from the **File** menu (choose **File** > **Wizard**).

   
   VMware GSX Server
To run VMware software, you must first configure a virtual machine.
Run the Configuration Wizard.
Run the Configuration Editor.
Open an existing configuration.
For new users, the configuration wizard is the easiest way to create a virtual machine.
You may also select a recently used configuration:
OK
Exit
Cancel

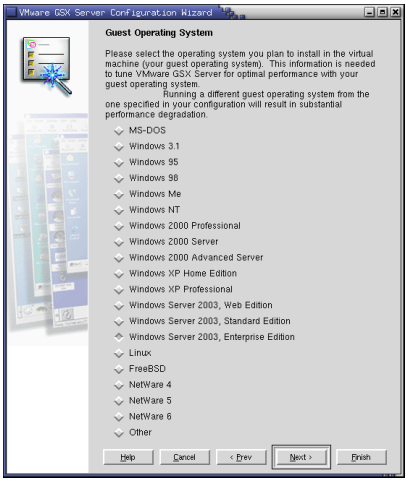
   The Configuration Wizard presents you with a series of screens that you navigate using the **Next** and **Prev** buttons at the bottom of each screen. At each screen, follow the instructions, then click **Next** to proceed to the next screen.

4. The Welcome screen appears.


VMware GSX Server Configuration Wizard
Welcome
Welcome to the VMware GSX Server Configuration Wizard.
This wizard automates the most common tasks in order to properly create and configure a VMware GSX Server virtual machine. It will ask a few simple questions, and at the end it will create all the files you need to run the virtual machine.
The configuration settings which you will be selecting for the new virtual machine can be viewed and changed at a later time by using the Configuration Editor.
Click the "Next" button to proceed.
At any point you may return to the previous panel by clicking on the "Prev" button, or abort the wizard by clicking on the "Cancel" button. You may also select default parameters and skip to the last panel by using the "Finish" button.
The "Help" button provides context sensitive help and links to relevant online documentation.
Help
Cancel
< Prev
Next >
Finish

Click **Next** to begin creating your new virtual machine.

5. Select a guest operating system.

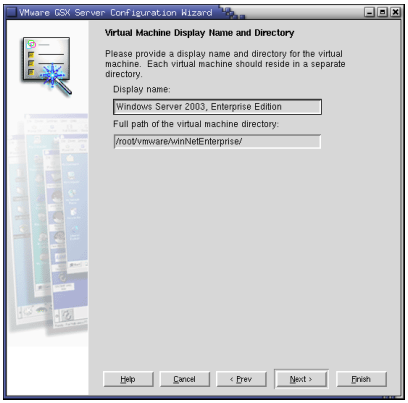

VMware GSX Server Configuration Wizard
Guest Operating System
Please select the operating system you plan to install in the virtual machine (your guest operating system). This information is needed to tune VMware GSX Server for optimal performance with your guest operating system.
Running a different guest operating system from the one specified in your configuration will result in substantial performance degradation.
MS-DOS
Windows 3.1
Windows 95
Windows 98
Windows Me
Windows NT
Windows 2000 Professional
Windows 2000 Server
Windows 2000 Advanced Server
Windows XP Home Edition
Windows XP Professional
Windows Server 2003, Web Edition
Windows Server 2003, Standard Edition
Windows Server 2003, Enterprise Edition
Linux
FreeBSD
NetWare 4
NetWare 5
NetWare 6
Other
Help
Cancel
< Prev
Next >
Finish

This screen asks which operating system you plan to install in the virtual machine. The Configuration Wizard uses this information to select appropriate default values, such as the amount of memory to allocate and disk space needed. The wizard also uses this information when naming associated virtual machine files.

If the operating system you are using is not listed, select **Other**.

You can find detailed installation notes for guest operating systems in Installing Guest Operating Systems on page 251.

6. Enter a directory and display name for the virtual machine.

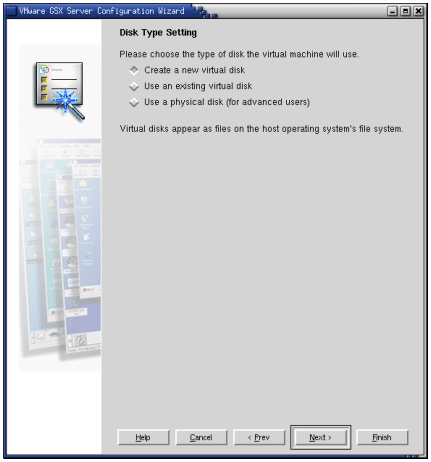

VMware GSX Server Configuration Wizard
Virtual Machine Display Name and Directory
Please provide a display name and directory for the virtual machine. Each virtual machine should reside in a separate directory.
Display name:
Windows Server 2003, Enterprise Edition
Full path of the virtual machine directory:
/root/vmware/winNetEnterprise/
Help
Cancel
< Prev
Next >
Finish

Enter a display name for the virtual machine or accept the default. The name specified here appears in the VMware Management Interface and the Connect to VMware Virtual Machine dialog box that appears when you connect to a virtual machine with the VMware Remote Console. It is also used as the name of the directory where the files associated with this virtual machine are stored.

Each virtual machine should have its own directory. All associated files, such as the configuration file and the disk file, are placed in this directory.

The default location is `<homedir>/vmware/<guestOS>`, where `<homedir>` is the home directory of the user who is currently logged on and `<guestOS>` is an abbreviation of the guest operating system you selected in the previous panel. If other users need to access this virtual machine, you should consider placing the virtual machine files in a location that is accessible to them. For more information, see Sharing Virtual Machines with Other Users on page 250.

7. Select the disk type.


VMware GSX Server Configuration Wizard
Disk Type Setting
Please choose the type of disk the virtual machine will use.
Create a new virtual disk
Use an existing virtual disk
Use a physical disk (for advanced users)
Virtual disks appear as files on the host operating system's file system.
Help
Cancel
< Prev
Next >
Finish

Select **Create a new virtual disk**.

Virtual disks are the best choice for most virtual machines. They are quick and easy to set up and can be moved to new locations on the same host computer or to different host computers. Virtual disks start as small files on the host computer's hard drive, then expand as needed — up to the size you specify in the next step.

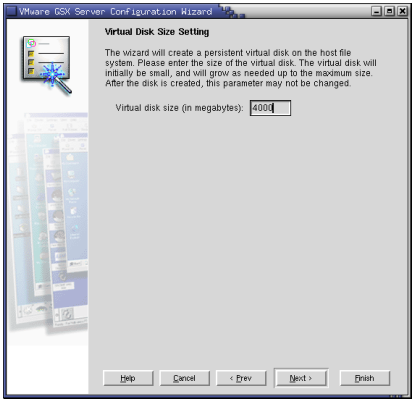
To use an existing virtual disk with this virtual machine, select **Use an existing virtual disk**.

To install your guest operating system directly on an existing IDE disk partition, read the reference note Installing an Operating System onto a Raw Partition from a Virtual Machine on page 396.

Caution: Raw disk configurations are recommended only for expert users.

To install the guest operating system on a raw IDE disk, select **Use a physical disk**. To use a raw SCSI disk, add it to the virtual machine later with the Configuration Editor. Booting from a raw SCSI disk is not supported.

8. Select the size of the virtual disk.


VMware GSX Server Configuration Wizard
Virtual Disk Size Setting
The wizard will create a persistent virtual disk on the host file system. Please enter the size of the virtual disk. The virtual disk will initially be small, and will grow as needed up to the maximum size. After the disk is created, this parameter may not be changed.
Virtual disk size (in megabytes):
4000
Help
Cancel
< Prev
Next >
Finish

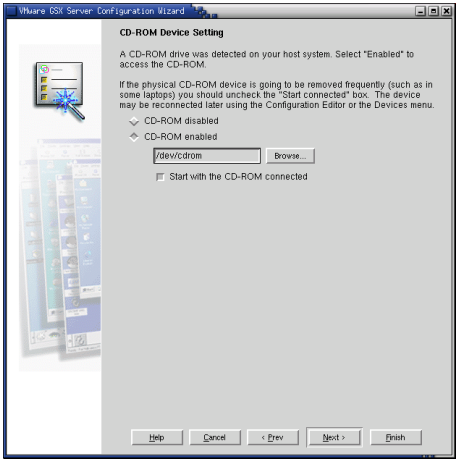
Enter the size of the virtual disk that you wish to create. Use the default of 4000 (megabytes, or 4GB) or change the setting. The maximum size is 128GB for an IDE virtual disk or 256GB for a SCSI virtual disk. When you specify the size of the virtual disk, that amount of disk space is not immediately occupied by the virtual disk file. The virtual disk file grows as needed when applications and files are added to them, until the virtual disk reaches the maximum capacity you specify here.

Note: If this setting is larger than the capacity of the host machine's hard disk, a warning message appears. You can ignore this message for now, as you can move this virtual machine to a drive that can hold it at a later time.

Make the Virtual Disk Big Enough

- The virtual disk should be large enough to hold the guest operating system and all of the software that you intend to install, with room for data and growth.
- You cannot change the virtual disk's maximum capacity later.
- You can install additional virtual disks using the Configuration Editor.
- For example, you need about 750MB of actual free space on the file system containing the virtual disk to install Windows 2000 and popular applications such as Microsoft Office inside the virtual machine. You can set up a single virtual disk to hold these files. Or you can split them up — installing the operating system on the first virtual disk and using a second virtual disk for applications or data files.

9. Enable the CD-ROM drive.


VMware GSX Server Configuration Wizard
CD-ROM Device Setting
A CD-ROM drive was detected on your host system. Select "Enabled" to access the CD-ROM.
If the physical CD-ROM device is going to be removed frequently (such as in some laptops) you should uncheck the "Start connected" box. The device may be reconnected later using the Configuration Editor or the Devices menu.
CD-ROM disabled
CD-ROM enabled
/dev/cdrom
Browse...
Start with the CD-ROM connected
Help
Cancel
< Prev
Next >
Finish

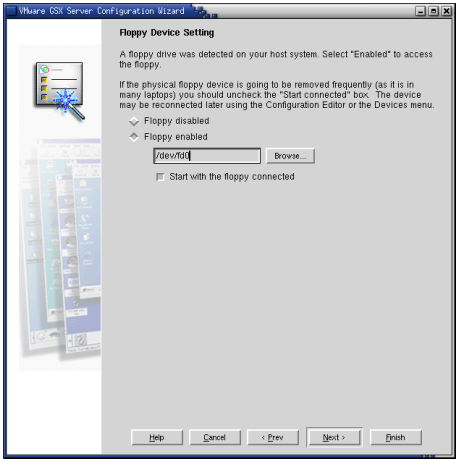
Most operating systems require the use of a CD-ROM for installation.

Select **CD-ROM enabled**. To enter the path to the CD-ROM drive, Click **Browse** or type the path to the CD-ROM drive. For example, `/dev/cdrom`.

If you wish, you can disable access to the CD-ROM drive later using the Configuration Editor (**Settings** > **Configuration Editor**) or from the **Devices** menu when your virtual machine is running.

In addition, choose whether you want the CD-ROM drive to be connected when you power on the virtual machine.

10. Enable the floppy disk drive.


VMware GSX Server Configuration Wizard
Floppy Device Setting
A floppy drive was detected on your host system. Select "Enabled" to access the floppy.
If the physical floppy device is going to be removed frequently (as it is in many laptops) you should uncheck the "Start connected" box. The device may be reconnected later using the Configuration Editor or the Devices menu.
Floppy disabled
Floppy enabled
/dev/fd0
Browse...
Start with the floppy connected
Help
Cancel
< Prev
Next >
Finish

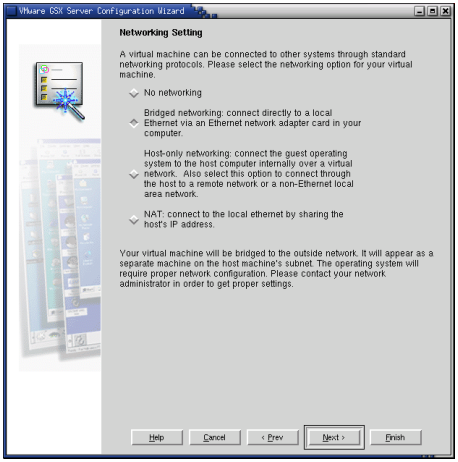
Select the **Floppy enabled** option. To enter the path to the floppy drive, click Browse or type the path to the physical floppy drive (for example, type `/dev/fd0`).

Some operating systems may require the use of a floppy drive during installation.

If you wish, you can disable access to the floppy drive later using the Configuration Editor (**Settings** > **Configuration Editor**) or from the **Devices** menu when your virtual machine is running.

In addition, choose whether you want the floppy drive to be connected when you power on the virtual machine.

11. Configure the networking capabilities of the virtual machine.


VMware GSX Server Configuration Wizard
Networking Setting
A virtual machine can be connected to other systems through standard networking protocols. Please select the networking option for your virtual machine.
No networking
Bridged networking: connect directly to a local Ethernet via an Ethernet network adapter card in your computer.
Host-only networking: connect the guest operating system to the host computer internally over a virtual network. Also select this option to connect through the host to a remote network or a non-Ethernet local area network.
NAT: connect to the local ethernet by sharing the host's IP address.
Your virtual machine will be bridged to the outside network. It will appear as a separate machine on the host machine's subnet. The operating system will require proper network configuration. Please contact your network administrator in order to get proper settings.
Help
Cancel
< Prev
Next >
Finish

To enable your virtual machine to use an existing Ethernet connection on your host computer, select **Bridged networking**.

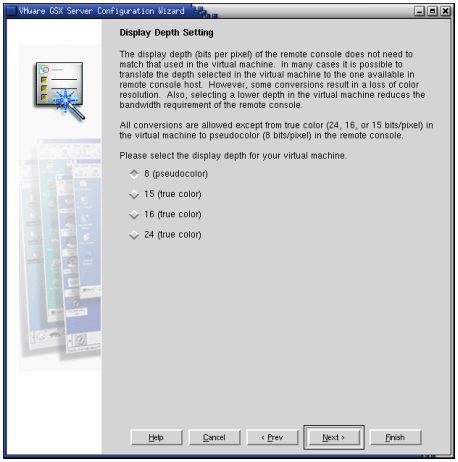
To enable your virtual machine to use a virtual network limited to the host and the virtual machines running on the host, select **Host-only networking**.

To enable your virtual machine to use both an existing Ethernet connection on your host computer and also a virtual network limited to the host and the virtual machines running on the host, select **Bridged and host-only networking**. This allows for the sharing of files between the virtual machine and the host operating system.

To give the virtual machine access to the host computer's dial-up or external network connection using the host's IP address, select **NAT**. NAT is useful if you have a wireless NIC on your host (as bridged networking is not supported on wireless NICs) and allows for the sharing of files between the virtual machine and the host operating system.

For more details about GSX Server networking options, see Networking on page 403.

12. Select the color depth for the virtual machine.

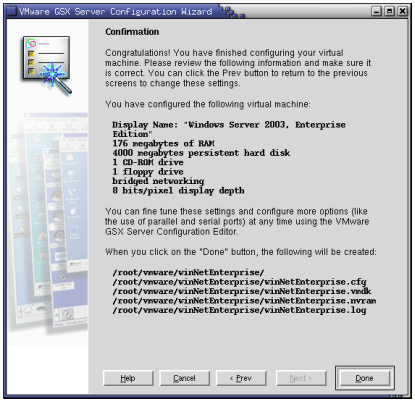

VMware GSX Server Configuration Wizard
Display Depth Setting
The display depth (bits per pixel) of the remote console does not need to match that used in the virtual machine. In many cases it is possible to translate the depth selected in the virtual machine to the one available in remote console host. However, some conversions result in a loss of color resolution. Also, selecting a lower depth in the virtual machine reduces the bandwidth requirement of the remote console.
All conversions are allowed except from true color (24, 16, or 15 bits/pixel) in the virtual machine to pseudocolor (8 bits/pixel) in the remote console.
Please select the display depth for your virtual machine.
8 (pseudocolor)
15 (true color)
16 (true color)
24 (true color)
Help
Cancel
< Prev
Next >
Finish

Select one of the following:

- 8 (pseudocolor) - 8 bits of colors (256 colors) minimizes network bandwidth usage, but it is a pseudo-color or color map mode, not a true color setting. 8 (pseudocolor) is the default setting.
- 15 (true color) - for true color resolution, at the expense of network bandwidth.
- 16 (true color) - for higher true color resolution, at the expense of even more network bandwidth.
- 24 (true color) - for the highest true color resolution, at the expense of the most network bandwidth.

A higher color depth setting slows down screen redraws when you use a remote console to view a virtual machine across a network connection. However, with greater color depth, you get better color resolution and fidelity, which may be an issue, depending on the applications you intend to run on the virtual machine.

13. Review and finish the configuration.


VMware GSX Server Configuration Wizard
Confirmation
Congratulations! You have finished configuring your virtual machine. Please review the following information and make sure it is correct. You can click the Prev button to return to the previous screens to change these settings.
You have configured the following virtual machine:
Display Name: "Windows Server 2003, Enterprise Edition"
176 megabytes of RAM
4000 megabytes persistent hard disk
1 CD-ROM drive
1 floppy drive
bridged networking
8 bits/pixel display depth
You can fine tune these settings and configure more options (like the use of parallel and serial ports) at any time using the VMware GSX Server Configuration Editor.
When you click on the "Done" button, the following will be created:
/root/vmware/winNetEnterprise/
/root/vmware/winNetEnterprise/winNetEnterprise.cfg
/root/vmware/winNetEnterprise/winNetEnterprise.vmdk
/root/vmware/winNetEnterprise/winNetEnterprise.nvram
/root/vmware/winNetEnterprise/winNetEnterprise.log
Help
Cancel
< Prev
Next >
Done

This screen presents all the options you selected. Review it for accuracy and click **Done** to complete the virtual machine configuration.

Note: The Configuration Wizard allocates a default amount of memory to the virtual machine. You can change this setting in the Configuration Editor (**Settings** > **Configuration Editor**).

Installing a Guest Operating System

Installing a guest operating system inside your GSX Server virtual machine is essentially the same as installing it on a physical computer. The basic steps for a typical operating system are:

1. Connect to the virtual machine with the local console.
2. Insert the installation CD-ROM or floppy disk for your guest operating system into the appropriate drive on your GSX Server host.
3. Power on your virtual machine — click the **Power On** button.
4. Follow the instructions provided by the operating system vendor.

The next section provides notes on installing a Windows 2000 guest operating system. The screen shots illustrate the process on a Windows host. The steps are the same on a Linux host.

For information on installing other guest operating systems, see Installing Guest Operating Systems on page 251.

Example: Installing Windows 2000 as a Guest Operating System

You can install Windows 2000 Professional, Server or Advanced Server in a virtual machine using the corresponding Windows 2000 distribution CD.

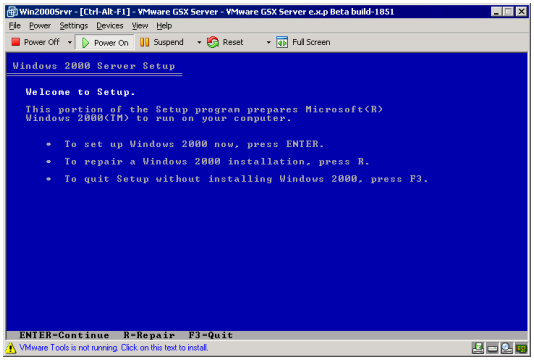
Note: Some Microsoft Windows 2000 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 2000 operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

Windows 2000 Installation Steps

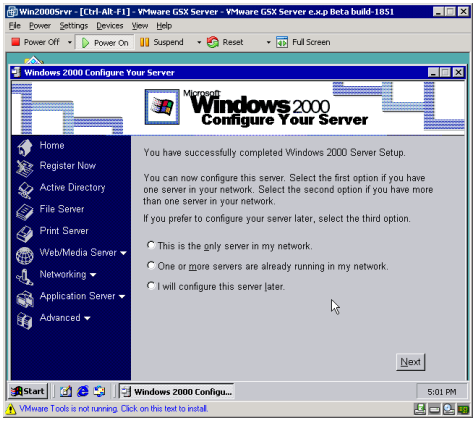
Follow these steps to install Windows 2000 as a guest operating system:

1. Use the Configuration Editor to verify the virtual machine's devices are set up as you expect. For example, if you would like networking software to be installed during the Windows 2000 installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 2000 CD in the CD-ROM drive on the server host.

3. Power on the virtual machine to start installing Windows 2000.


Win2000Srvr - [Ctrl-Alt-F1] - VMware GSX Server - VMware GSX Server e.x.p Beta build-1851
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
Windows 2000 Server Setup
Welcome to Setup.
This portion of the Setup program prepares Microsoft(R) Windows 2000(TM) to run on your computer.
• To set up Windows 2000 now, press ENTER.
• To repair a Windows 2000 installation, press R.
• To quit Setup without installing Windows 2000, press F3.
ENTER=Continue R=Repair F3=Quit
VMware Tools is not running. Click on this text to install.

4. If you enabled the virtual machine's Ethernet adapter, an AMD PCNET Family Ethernet Adapter is detected and set up automatically.
5. Follow the installation steps as you would for a physical computer.


Win2000Srvr - [Ctrl-Alt-F1] - VMware GSX Server - VMware GSX Server e.x.p Beta build-1851
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
Windows 2000 Configure Your Server
Microsoft Windows 2000 Configure Your Server
Home
Register Now
Active Directory
File Server
Print Server
Web/Media Server
Networking
Application Server
Advanced
You have successfully completed Windows 2000 Server Setup.
You can now configure this server. Select the first option if you have one server in your network. Select the second option if you have more than one server in your network.
If you prefer to configure your server later, select the third option.
This is the only server in my network.
One or more servers are already running in my network.
I will configure this server later.
Next
Start
Windows 2000 Configu...
5:01 PM
VMware Tools is not running. Click on this text to install.

After installing your guest operating system, you are ready to install VMware Tools as described in Installing VMware Tools on page 113. After you install VMware Tools, you need to change your Windows 2000 screen area to be greater than 640x480 pixels; if you do not change it, Windows 2000 uses the standard VGA driver, and your performance will suffer.

For more information about Windows 2000 guest operating systems — like enabling networking or sound in the virtual machine, see Windows 2000 Installation Guidelines on page 263.

5

Using VMware Tools

Using VMware Tools

The following sections describe how to install and run VMware Tools:

- About VMware Tools on page 111
- Installing VMware Tools on page 113
- Executing Scripts When the Virtual Machine's Power State Changes on page 122
- Configuring VMware Tools on page 124
- About the VMware Guest Operating System Service on page 136

About VMware Tools

It is very important that you install VMware Tools in the guest operating system. Although VMware GSX Server can run a guest operating system without VMware Tools, you lose out on important functionality and convenience.

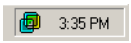
When you install VMware Tools, you install

- The VMware SVGA driver.
- The VMware guest operating system service (or guest service).
- The VMware Tools control panel.
- A set of scripts that can run when the virtual machine's power state changes.

With the VMware SVGA driver installed, GSX Server supports up to 32-bit displays and high display resolution, with significantly faster overall graphics performance. If you run a guest operating system without VMware Tools, the graphics environment within the virtual machine is limited to VGA mode graphics (640x480, 16 color) and display performance may be unsatisfactory.

The VMware guest operating system service performs various duties within the guest operating system, such as passing messages from the host operating system to the guest operating system, sending a heartbeat to GSX Server and synchronizing the time in the guest operating system with the time in the host operating system. The guest service starts automatically when the guest operating system boots. See About the VMware Guest Operating System Service on page 136.

In a Windows guest, you can access the VMware Tools control panel through the Windows Control Panel (choose **Start** > **Settings** > **Control Panel** > **VMware Tools**) or via the VMware Tools icon, which appears by default in the system tray.



In a Linux or FreeBSD guest operating system, the VMware Tools control panel is called `vmware-toolbox`. It can be launched manually as a background process from a terminal using

```
vmware-toolbox &
```

In a NetWare 5.1 or 6.0 guest operating system, you can access the VMware Tools control panel by choosing **Novell** > **Settings** > **VMware Tools for NetWare**.

In a NetWare 4.2 guest operating system, you can use VMware Tools commands in the system console. The VMware Tools program is called `vmwtool`. For information

about using this command, see Configuring VMware Tools for NetWare Guests in the System Console on page 133.

With some window managers, you can place the command to start VMware Tools in a startup configuration so VMware Tools starts automatically when you start your graphical environment. Consult your window manager's documentation for details.

Installation files for VMware Tools for all supported Windows, Linux, NetWare and FreeBSD guest operating systems are built into GSX Server.

Installing VMware Tools

The installer for VMware Tools is built into GSX Server as an ISO image file. An ISO image file looks like a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer. You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file.

When you choose **Settings** > **VMware Tools Install** from a console window, GSX Server temporarily connects the virtual machine's first virtual CD-ROM drive to the ISO image file that contains the VMware Tools installer for your guest operating system and begins the installation process. (If you decide not to proceed with the installation, choose **Settings** > **Cancel VMware Tools Install** to return your virtual machine's CD-ROM drive to its original configuration.)

Don't Forget VMware Tools

- It is very important that you install VMware Tools in the guest operating system. If you do not install VMware Tools, the graphics environment within the virtual machine is limited to VGA mode graphics (640x480, 16 color).
- With the VMware Tools SVGA driver installed, VMware GSX Server supports up to 32-bit displays and high display resolution, with significantly faster overall graphics performance.
- Other tools in the package support time synchronization between host and guest, automatic grab and release of the mouse cursor, copying and pasting between guest and host, and improved mouse performance in some guest operating systems.

Installing VMware Tools in a Windows Virtual Machine

VMware Tools for Windows guest operating systems supports Windows 95, Windows 98, Windows Me, Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003.

The details of how you install VMware Tools depends on the version of Windows you are running. The following steps show how to install VMware Tools in a Windows 2000 guest operating system. Some steps that are automated in newer versions of Windows must be performed manually in Windows 9x and Windows NT.

Note: If you are running GSX Server for Windows and your virtual machine has only one CD-ROM drive, the CD-ROM drive must be configured as an IDE or SCSI CD-ROM drive. It cannot be configured as a generic SCSI device.

To add an IDE or SCSI CD-ROM drive, see Adding, Configuring and Removing Devices in a Virtual Machine on page 237. For information about generic SCSI, see Connecting to a Generic SCSI Device on page 517.

Installing VMware Tools in a Windows Guest Operating System

1. Power on the virtual machine.
2. When the guest operating system starts, prepare your virtual machine to install VMware Tools.

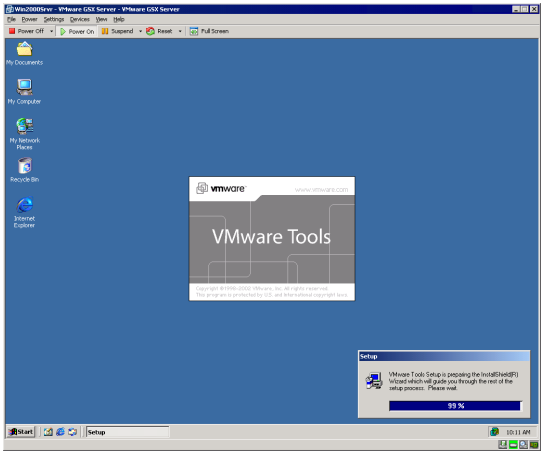
   Choose **Settings** > **VMware Tools Install**.

   The remaining steps take place inside the virtual machine.

3. If you have auto-run enabled in your guest operating system (the default setting for Windows operating systems), a dialog box appears after a few seconds. It asks if you want to install VMware Tools. Click **Yes** to launch the InstallShield wizard.

   If autorun is not enabled, the dialog box does not appear automatically. If it does not appear, run the VMware Tools installer. Click **Start** > **Run** and enter `D:\setup\setup.exe` where `D:` is your first virtual CD-ROM drive.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The GSX Server software contains an ISO image that looks like a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer. This image contains all the files needed to install VMware Tools in your guest operating system. When you finish installing VMware Tools, this image file no longer appears in your CD-ROM drive.



4. Follow the on-screen instructions.
5. On Windows Me, Windows 2000, Windows XP and Windows Server 2003 guests, the SVGA driver is installed automatically and the guest operating system uses it after it reboots.

Additional Steps for Some Versions of Windows When Migrating from Old Disk Versions

If you are migrating a GSX Server 1 disk to GSX Server 2 and your guest operating system is Windows NT, Windows Me, Windows 98 or Windows 95, you need to configure the video driver by hand. Instructions open automatically in Notepad at the

end of the installation process. If the Notepad window is hidden, bring it to the front by clicking the **Notepad** button on the Windows taskbar.

For details, see the steps that correspond to your guest operating system.

Windows NT

1. After installing VMware Tools, click **Finish**. The Display Properties dialog box appears.
2. Click the **Display Type** button. The Display Type dialog box appears.
3. Click the **Change** button. The Change Display dialog box appears.
4. Select **VMware, Inc.** from the **Manufacturer** list.
5. Select **VMware SVGA II** as the display adapter and click **OK**.
6. Click **Yes** in response to the on-screen question about third-party drivers to install the driver, then click **OK** to confirm the drivers were installed.
7. Click **Close** from the Display Type dialog box, then click **Close** from the Display Properties dialog box.
8. Click **Yes** to restart Windows NT and start using the new video driver.
9. The VMware Tools background application is launched automatically when you reboot your virtual machine.

Windows Me

1. After installing VMware Tools, click **Finish**. The Display Settings dialog box appears.
2. Click the **Advanced** button.
3. Click the **Adapter** tab.
4. Click the **Change** button. This starts the Update Device Driver Wizard.
5. The wizard presents two options. Choose the second option to **Specify the location of the driver**.

   Click **Next**.
6. Check the **Specify a location** checkbox. Enter the following path:

   `D:\video\win9x`

   `D:` is the drive letter for the first virtual CD-ROM drive in your virtual machine.

   Click **OK**.
7. Windows Me automatically locates your driver.
8. Select the **VMware SVGA II** display adapter and click **Next**.

9. Click **Next** to install the driver.

   If you are upgrading a virtual machine created under GSX Server 1, you may see a dialog box that warns, "The driver you are installing is not specifically designed for the hardware you have.… Do you wish to continue?" Click **Yes**.

   After the driver is installed, click **Finish**.

10. Click **Yes** to restart Windows Me and start using the new video driver.
11. The VMware Tools background application starts automatically when you reboot your virtual machine.

Windows 98

1. After installing VMware Tools, click **Finish**. The Display Settings dialog box appears.
2. Click the **Advanced** button. The Standard Display Adapter (VGA) Properties dialog box appears. If you are upgrading from a previous version of the VMware drivers, this dialog box is titled VMware SVGA Properties.
3. Click the **Adapter** tab.
4. Click the **Change** button. This starts the Update Device Driver Wizard. Click **Next**.
5. The wizard presents two options. Choose the option to **Display a list of all drivers in a specific location**. Click **Next**.
6. Select **Have Disk**. The Install From Disk dialog box appears.
7. Enter the following path:

   `D:\video\win9x`

   `D:` is the drive letter for the first virtual CD-ROM drive in your virtual machine.

   Click **OK**.

8. Select **VMware SVGA II** display adapter and click **OK**.
9. Answer **Yes** to the on-screen question, then click **Next** to install the driver. After the driver is installed, click **Finish**.
10. Click **Close** in the SVGA Properties dialog box, then click **Close** in the Display Settings dialog box.
11. Click **Yes** to restart Windows 98 and start using the new video driver.
12. The VMware Tools background application starts automatically when you reboot your virtual machine.

Windows 95

1. After installing VMware Tools, click **Finish**. The Display Settings dialog box appears.
2. Click the **Advanced Properties** button. The Advanced Display Properties dialog box appears.
3. Click the **Change** button. The Select Device dialog box appears.
4. Select **Have Disk**.
5. Enter the following path:

   `D:\video\win9x`

   `D:` is the drive letter for the first virtual CD-ROM drive in your virtual machine.

   Click **OK**.
6. Click **OK** again to install the driver.
7. Click **Close** from the Advanced Display Properties dialog box, then click **Close** from the Display Setting dialog box.
8. Click **Yes** to restart Windows 95 and start using the new video driver.
9. The VMware Tools background application starts automatically when you reboot your virtual machine.

Installing VMware Tools in a Linux Virtual Machine

1. Power on the virtual machine.
2. After the guest operating system has started, prepare your virtual machine to install VMware Tools.

   Choose **Settings** > **VMware Tools Install**.

   The remaining steps take place inside the virtual machine.
3. As root, open a terminal, mount the VMware Tools virtual CD-ROM image, copy its contents to `/tmp`, then unmount it.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The GSX Server software contains an ISO image that looks like a CD-ROM to your guest operating system. This image contains all the files needed to install VMware Tools in your guest operating system.

   Note: Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom`, modify the following commands to reflect the conventions used by your distribution.

Note: Some Linux distributions automatically mount CD-ROMs. If your distribution uses automounting, do not use the `mount` and `umount` commands below. You still must copy the VMware Tools installer.

```
mount -t iso9660 /dev/cdrom /mnt
cp /mnt/vmware-linux-tools.tar.gz /tmp
umount /dev/cdrom
```

4. Untar the VMware Tools tar file in `/tmp`, and install it.

```
cd /tmp
tar zxf vmware-linux-tools.tar.gz
cd vmware-linux-tools
./install.pl
```

5. Start X and your graphical environment if they are not started yet.
6. In an X terminal, launch the VMware Tools background application.

```
vmware-toolbox &
```

You may run VMware Tools as root or as a normal user. To shrink virtual disks, you should run VMware Tools as root (`su -`).

Starting VMware Tools Automatically

You may find it helpful to configure your guest operating system so VMware Tools starts when you start your X server. The steps for doing so vary depending on your Linux distribution and the desktop environment you are running. Check your operating system documentation for the appropriate steps to take.

For example, in a Red Hat Linux 7.1 guest using GNOME, follow these steps.

1. Open the Startup Programs panel in the GNOME Control Center.

   Main Menu (the foot icon in the lower left corner of the screen) > Programs > Settings > Session > Startup Programs
2. Click Add.
3. In the Startup Command field, enter `vmware-toolbox`.
4. Click OK, click OK again, then close the GNOME Control Center.

The next time you start X, VMware Tools starts automatically.

Installing VMware Tools in a FreeBSD Virtual Machine

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools.

   Choose Settings > VMware Tools Install.

The remaining steps take place inside the virtual machine.

3. As root, open a terminal, mount the VMware Tools virtual CD-ROM image, copy its contents to `/tmp`, then unmount it.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The GSX Server software contains an ISO image that looks like a CD-ROM to your guest operating system. This image contains all the files needed to install VMware Tools in your guest operating system.

   Note: Some FreeBSD distributions automatically mount CD-ROMs. If your distribution uses automounting, do not use the `mount` and `umount` commands below. You still must copy the VMware Tools installer.

   ```
   mount /cdrom
   cp /cdrom/vmware-freebsd-tools.tar.gz /tmp
   umount /cdrom
   ```

4. Untar the VMware Tools tar file in `/tmp`, and install it.

   ```
   cd /tmp
   tar zxf vmware-freebsd-tools.tar.gz
   cd vmware-freebsd-tools
   ./install.pl
   ```

5. Start X and your graphical environment if they are not started yet.

6. In an X terminal, launch the VMware Tools background application.

   ```
   vmware-toolbox &
   ```

You may run VMware Tools as root or as a normal user. To shrink virtual disks, you should run VMware Tools as root (`su -`).

Note: In a FreeBSD 4.5 guest operating system, sometimes VMware Tools does not start after you install VMware Tools, reboot the guest operating system or start VMware Tools on the command line in the guest. An error message appears:

```
Shared object 'libc.so.3' not found.
```

The required library was not installed. This does not happen with full installations of FreeBSD 4.5, but does occur for minimal installations. To fix the problem of the missing library, complete the following steps:

1. Insert and mount the FreeBSD 4.5 installation CD or access the ISO image file.

2. Change directories and run the install script.

   ```
   cd /cdrom/compat3x
   ./install.sh
   ```

Installing VMware Tools in a NetWare Virtual Machine

VMware Tools is available for NetWare 4.2, 5.1, 6.0 and 6.5 guest operating systems.

When you install VMware Tools in a NetWare guest operating system, the CPU idler program is installed and loaded automatically. The idler can be disabled from the system console. For information on configuring VMware Tools from the system console, see Configuring VMware Tools for NetWare Guests in the System Console on page 133.

Follow the appropriate steps for your NetWare guest operating system.

- Installing VMware Tools in a NetWare 5.1, 6.0 or 6.5 Virtual Machine on page 120
- Installing VMware Tools in a NetWare 4.2 Virtual Machine on page 120

Installing VMware Tools in a NetWare 5.1, 6.0 or 6.5 Virtual Machine

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools. Choose **Settings** > **VMware Tools Install**. The remaining steps take place inside the virtual machine.

   If you are installing VMware Tools in a NetWare 6.5 virtual machine, skip to step 4.
3. Load the `CD9660.NSS` driver so the CD-ROM device mounts the ISO image as a volume. In the system console, type
   ```
   load CD9660.NSS
   ```
4. When the driver finishes loading you can begin installing VMware Tools. In the system console, type
   ```
   vmwtools:\setup.ncf
   ```
   When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Logger Screen (NetWare 6.0 guests) or the Console Screen (NetWare 5.1 guests).
5. Restart the guest operating system. In the system console, type
   ```
   restart server
   ```

Installing VMware Tools in a NetWare 4.2 Virtual Machine

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools. Choose **Settings** > **VMware Tools Install**. The remaining steps take place inside the virtual machine.
3. Load the `cdrom.nlm` module. In the system console, type
   ```
   load cdrom
   ```

4. Mount the VMware Tools CD-ROM image. In the system console, type
   `cd mount vmwtools`
5. Start installing VMware Tools. In the system console, type
   `vmwtools:\setup`

   When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Console Screen.
6. Bring the guest operating system down. In the system console, type
   `down`
7. Restart the guest operating system. In the system console, type
   `restart server`

Executing Scripts When the Virtual Machine's Power State Changes

You can run scripts in the guest operating system when you change the power state of a virtual machine; that is, when you power on, power off, suspend or resume the virtual machine.

Scripts can help automate guest operating system operations when you change the virtual machine's power state.

Note: There are no scripts for FreeBSD and NetWare guest operating systems.

You perform these power operations from the toolbar buttons and menus in the consoles. For more information on changing the power state of a virtual machine in a console, see Special Power Options for Virtual Machines on page 195.

Scripts can run when using the power buttons in the VMware Management Interface. For more information, see Changing the Power State of a Virtual Machine on page 168.

Scripts can be executed only when the VMware guest operating system service is running. The guest service starts by default when you start the guest operating system. For more information about the guest service, see About the VMware Guest Operating System Service on page 136.

Default scripts are included in VMware Tools. On a Windows host, provided the virtual machine is configured to use DHCP, the default script executed when suspending a virtual machine releases the IP address of the virtual machine while the default script executed when resuming a virtual machine renews the IP address of the virtual machine. On a Linux host, the default script executed when suspending a virtual machine stops networking for the virtual machine while the default script executed when resuming a virtual machine starts networking for the virtual machine.

In addition, you can create your own scripts. The scripts you can run must be batch files for Windows hosts but can be any executable format (such as shell or Perl scripts) for Linux hosts. You should have a thorough familiarity with these types of scripts before you modify the default scripts or create your own.

If you create your own scripts, you must associate each script with its particular power operation. For more information, see Choosing Scripts for VMware Tools to Run During Power State Changes on page 125 for Windows guests and Choosing Scripts for VMware Tools to Run During Power State Changes on page 129 for Linux guests.

In order for scripts and their associated power operations to work, the following conditions must be met:

1. The VMware guest operating system service must be running in the virtual machine.
2. The version of VMware Tools must be updated to the current version. If you are using a virtual machine created with an older version of GSX Server or another older VMware product, update VMware Tools to the version included in this release.
3. Depending upon the operation the script performs, the virtual machine must have a virtual network adapter connected, otherwise the power operation fails.

Issues to Consider

Caution: When you reinstall VMware Tools after you upgrade the GSX Server software, any changes you made to the default scripts are overwritten. Any scripts you created on your own remain untouched, but do not benefit from any underlying changes that enhance the default scripts.

Note: Scripts cannot be run in Windows 95, NetWare and FreeBSD guest operating systems.

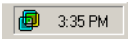
Note: All default scripts in Windows NT and Windows Me guest operating systems do not release and renew the IP address. To release and renew an IP address in a Windows NT or Windows Me guest operating system, you can create custom scripts.

Configuring VMware Tools

Configuring VMware Tools in a Windows Virtual Machine

This section shows the options available in a Windows guest operating system. Similar configuration options are available in VMware Tools for other guest operating systems.

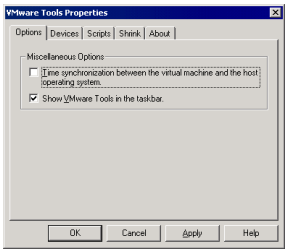
To open the VMware Tools control panel, double-click the **VMware Tools** icon in the system tray.



If the VMware Tools icon is not displayed in the system tray, choose **Start** > **Settings** > **Control Panel** > **VMware Tools**.

Setting Options with VMware Tools

The **Options** tab shows miscellaneous options.



- Time synchronization between the virtual machine and the host operating system

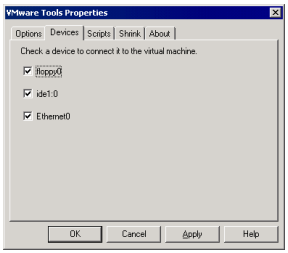
  This option lets you synchronize the time in the guest operating system with the time in the host operating system.

  Note: You can synchronize the time in the guest operating system with the time in the host operating system only when the time in the guest is earlier than the time in the host.

- Show VMware Tools in the taskbar

Connecting Devices with VMware Tools

The **Devices** tab allows you to enable or disable removable devices. Removable devices include the floppy and CD-ROM drives and the virtual network adapter.



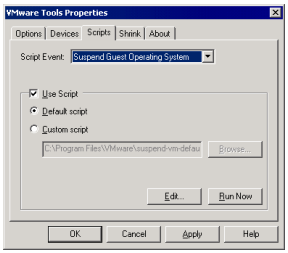
To connect a device, check the check box next to the device. To disconnect the device, uncheck the check box next to the device.

Note: You can also set these options from the **Devices** menu in the virtual machine window.

Choosing Scripts for VMware Tools to Run During Power State Changes

Through VMware Tools, you can run scripts that execute when you power on, power off, suspend or resume the virtual machine. For more information, see Executing Scripts When the Virtual Machine's Power State Changes on page 122.

Note: The **Scripts** tab does not appear in a Windows 95 guest operating system, as scripts cannot be run in a Windows 95 guest operating system.



A default script for each power state is included in VMware Tools. These scripts are located in the guest operating system in `C:\Program Files\VMware`.

When You …	This Default Script Runs
Suspend the guest operating system	`suspend-vm-default.bat`

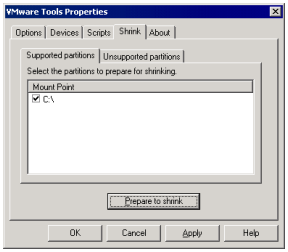
When You …	This Default Script Runs
Resume the guest operating system	`resume-vm-default.bat`
Power off the guest operating system	`poweroff-vm-default.bat`
Power on the guest operating system	`poweron-vm-default.bat`

For each power state, you can use the default script or you can substitute a script you created. In addition, you can test a script or disable the running of a script. Complete the following steps.

1. In the **Script Event** list, select the power operation with which to associate the script.
2. Do one of the following:
   - To select a different script, click **Custom Script**, then click **Browse** and select the new script.
   - To edit a script, click **Edit**. The script opens in your default editor. Make your changes there.
   - To test the script, click **Run Now**.
   - To disable the running of a script, uncheck the **Use Script** check box.
3. Click **Apply** to save your settings.

Shrinking Virtual Disks with VMware Tools

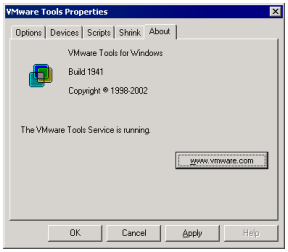
The **Shrink** tab gives you access to the controls you need if you wish to reclaim unused space in a virtual disk.



For more information about shrinking virtual disks, see Defragmenting and Shrinking Virtual Disks on page 374.

Viewing Information About VMware Tools

For general information about VMware Tools, click the **About** tab.



This tab contains the following information:

- The VMware Tools build number, which lets you verify your VMware Tools version matches the GSX Server version you are running and is useful when you request support.
- An indication as to whether the VMware guest operating system service is running.
- A button you click to visit the VMware Web site.

Configuring VMware Tools in a Linux or FreeBSD Virtual Machine

This section shows the options available in a Linux or FreeBSD guest operating system.

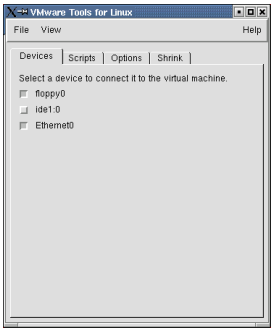
To open the VMware Tools control panel, at a command prompt, type:

```
vmware-toolbox &
```

You may run VMware Tools as root or as a normal user. To shrink virtual disks, you should run VMware Tools as root (`su -`).

Connecting Devices with VMware Tools

The **Devices** tab allows you to enable or disable removable devices. Removable devices include the floppy and CD-ROM drives and the virtual network adapter.



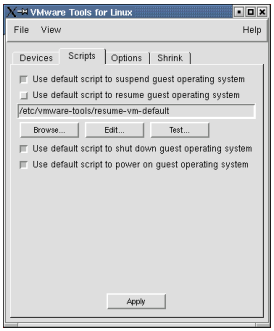
To connect a device, check the check box next to the device. To disconnect the device, uncheck the check box next to the device.

Note: You can also set these options from the **Devices** menu in the virtual machine window.

Choosing Scripts for VMware Tools to Run During Power State Changes

Through VMware Tools, you can run scripts that execute when you power on, power off, suspend or resume the virtual machine. For more information, see Executing Scripts When the Virtual Machine's Power State Changes on page 122.

Note: Scripts cannot be run in a FreeBSD guest operating system.



A default script for each power operation is included in VMware Tools. These scripts are located in the guest operating system in `/etc/vmware-tools`.

When You …	This Default Script Runs
Suspend the guest operating system	`suspend-vm-default`
Resume the guest operating system	`resume-vm-default`
Power off the guest operating system	`poweroff-vm-default`
Power on the guest operating system	`poweron-vm-default`

For each power state, you can use the default script or you can substitute a script you created. In addition, if you are logged in as root, you can test a script or disable the running of a script. Complete the following steps.

1. Select the appropriate power operation. Uncheck **Use default script to suspend guest operating system**, **Use default script to resume guest operating system**, **Use default script to shut down guest operating system** or **Use default script to power on guest operating system**.
2. Do one of the following:
   - To select a different script, click **Browse** and select the new script.

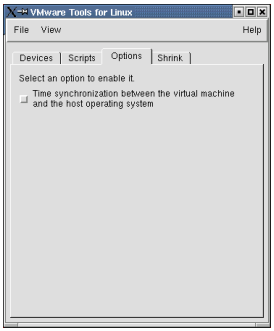
- To edit a script, click **Edit**. The script opens in your default editor. Make your changes there.
- To test a script, click **Test**.

  Note: If you plan to test scripts in a Turbolinux 7.0 guest operating system, you need to update the Turbolinux guest operating system. This is a known issue with Turbolinux. Go to *ftp://ftp.turbolinux.com/pub/turbolinux-updates/7.0/RPMS/initscripts-7.0.0-18.i586.rpm*.
- To disable a script, select the path to the script and delete it.

3. Click **Apply** to save your settings.

Setting Options with VMware Tools

The **Options** tab shows one miscellaneous option.


VMware Tools for Linux
File View Help
Devices Scripts Options Shrink
Select an option to enable it.
Time synchronization between the virtual machine and the host operating system

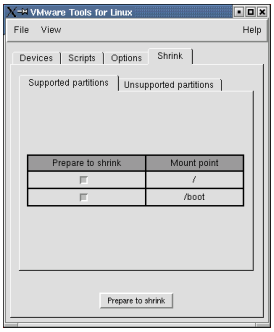
- Time synchronization between the virtual machine and the host operating system

  This option lets you synchronize the time in the guest operating system with the time in the host operating system.

  Note: You can synchronize the time in the guest operating system with the time in the host operating system only when the time in the guest is earlier than the time in the host.

Shrinking Virtual Disks with VMware Tools

The **Shrink** tab gives you access to the controls you need if you wish to reclaim unused space in a virtual disk.



To shrink virtual disks, you should run VMware Tools as the root user (`su -`). This way, you ensure the whole virtual disk is shrunk. Otherwise, if you shrink the virtual disk as a non-root user, you cannot prepare to shrink the parts of the virtual disk that require root-level permissions.

For more information about shrinking virtual disks, see Defragmenting and Shrinking Virtual Disks on page 374.

Configuring VMware Tools in a NetWare Virtual Machine

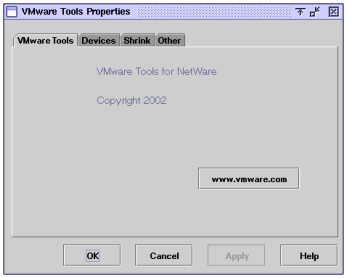
This section shows the options available in a NetWare 6.0 or 5.1 guest. Since there is no graphical user interface for NetWare 4.2, there is no VMware Tools control panel as there is for NetWare 6.0 or 5.1 guests. You can configure certain virtual machine options such as time synchronization, CPU idling and device configuration with VMware Tools in a NetWare 4.2 guest in the system console. For more information, see Configuring VMware Tools for NetWare Guests in the System Console on page 133.

Configuring VMware Tools in a NetWare 6.0 or NetWare 5.1 Guest

To open the VMware Tools control panel, choose **Novell** > **Settings** > **VMware Tools for NetWare**.

Viewing Information About VMware Tools

For general information about VMware Tools, click the **VMware Tools** tab.

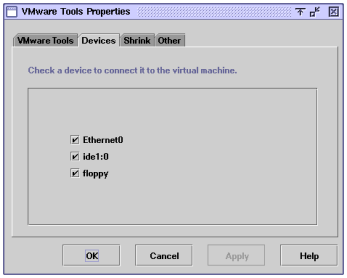


This tab contains:

- Copyright information.
- A button you click to visit the VMware Web site.

Connecting Devices with VMware Tools

The **Devices** tab allows you to enable or disable removable devices. Removable devices include the floppy and CD-ROM drives and the virtual network adapter.

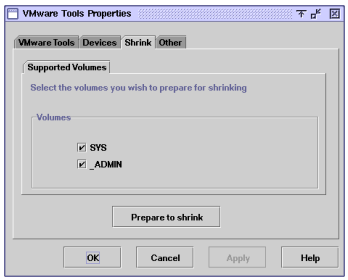


To connect a device, check the check box next to the device. To disconnect the device, uncheck the check box next to the device.

Note: You can also set these options from the **Devices** menu in the virtual machine window.

Shrinking Virtual Disks with VMware Tools

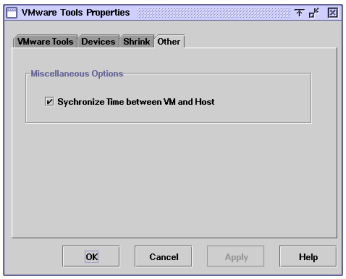
The **Shrink** tab gives you access to the controls you need if you wish to reclaim unused space in a virtual disk.



For more information about shrinking virtual disks, see Defragmenting and Shrinking Virtual Disks on page 374.

Setting Options with VMware Tools

The **Other** tab gives you the option to synchronize the time in the guest operating system with the time in the host operating system.



Note: You can synchronize the time in the guest operating system with the time in the host operating system only when the time in the guest is earlier than the time in the host.

Note: This feature does not work with NetWare 6.0 virtual machines. This issue may be resolved in the next NetWare 6.0 support pack that Novell will release.

Configuring VMware Tools for NetWare Guests in the System Console

You can configure certain virtual machine options such as time synchronization, CPU idling and device configuration with VMware Tools in a NetWare virtual machines in the system console. The VMware Tools command line program is called `vmwtool`. To

see the options associated with this command, at the system console, type `vmwtool help`

When VMware Tools is installed in a NetWare guest, a heartbeat is always sent from the virtual machine to GSX Server. You can verify the virtual machine's heartbeat by viewing information about this virtual machine in the VMware Management Interface. For more information, see Monitoring the Virtual Machine's Heartbeat on page 168.

In addition, you can gracefully power the virtual machine on or off in the management interface. To power a virtual machine on or off with the management interface, see Changing the Power State of a Virtual Machine on page 168. Since there are no scripts for NetWare virtual machines, no scripts are run.

Summary of VMware Tools Commands for a NetWare Guest

Each command in the following table must be entered into the system console after the VMware Tools command `vmwtool`. For example `vmwtool <command>`

`vmwtool` **Command**	**Definition**
`help`	Displays a summary of VMware Tools commands and options in a NetWare guest.
`partitonlist`	Displays a list of all disk partitions in the virtual disk and whether or not a partition can be shrunk.
`shrink <partition>`	Shrinks the listed partitions. If no partitions are specified, then all partitions in the virtual disk are shrunk. The status of the shrink process appears at the bottom of the system console. For more information, see Defragmenting and Shrinking Virtual Disks on page 374.
`devicelist`	Lists each removable device in the virtual machine, its device ID and whether the device is enabled or disabled. Removable devices include the virtual network adapter, CD-ROM and floppy drives.
`disabledevice <device name>`	Disables the specified device or devices in the virtual machine. If no device is specified, then all removable devices in the virtual machine are disabled. **Note:** You can also disable devices from the Devices menu in the virtual machine console window.

`vmwtool` **Command**	**Definition**
`enabledevice <device name>`	Enables the specified device or devices in the virtual machine. If no device is specified, then all removable devices in the virtual machine are enabled. **Note:** You can also disable devices from the Devices menu in the virtual machine console window.
`synctime [on|off]`	Lets you turn on or off time synchronization of the guest operating system with the host operating system. By default, time synchronization is turned off. Use this command without any options to view the current time synchronization status. You can synchronize the time in the guest operating system with the time in the host operating system only when the time in the guest is earlier than the time in the host.
`idle [on|off]`	Lets you turn on or off the CPU idler. By default, the idler is turned on. The CPU idler program is included in VMware Tools for NetWare guests. The idler program is needed because NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy.

About the VMware Guest Operating System Service

When you install VMware Tools in a virtual machine, the VMware guest operating system service is one of the primary components installed. The guest service can do the following:

- Synchronize the time of the guest operating system with the time in the host operating system.
- Run scripts in a virtual machine when the power state changes. See Executing Scripts When the Virtual Machine's Power State Changes on page 122.
- Execute commands in the virtual machine when you shut down or restart the guest operating system.
- Send a heartbeat to GSX Server so that it knows the guest operating system is running. A gauge for this heartbeat appears in the VMware Management Interface. For more information, see Using the Status Monitor on page 165.
- Pass information from the host operating system to the guest operating system.
- Pass information between the guest operating system and a VMware Scripting API script.

The guest service starts automatically when you boot the guest operating system.

In a Windows guest, the guest service program file is called `VMwareService.exe`. Help is available by right-clicking the VMware Tools icon in the system tray and choosing **Help**.

In a Linux guest, the guest service is called `vmware-guestd`. To display help about the guest service, including a list of all options, use the following command:

```
/etc/vmware/vmware-guestd --help
```

Synchronizing the Time in the Guest with the Host Operating System

The guest service can synchronize the date and time in the guest operating system with the time in the host operating system once every minute. To enable time synchronization for a Windows guest, see Setting Options with VMware Tools on page 124. To enable time synchronization for a Linux or FreeBSD guest, see Setting Options with VMware Tools on page 130. To enable time synchronization for a NetWare guest, see Setting Options with VMware Tools on page 133.

If you want to change the time synchronization setting without using the VMware Tools control panel, you can set the configuration file option `tools.syncTime` to `TRUE` or `FALSE` to enable or disable time synchronization.

In addition, the guest service can synchronize the date and time in the guest with the time in the host in response to various system events; for example, when you resume from disk. You can disable this in the configuration file by setting `time.synchronize.resume.disk = FALSE`

Executing Commands After You Power Off or Reset a Virtual Machine

In a Linux guest, you can have the guest service execute specific commands when you shut down or restart the guest operating system. This is in addition to any script that you may have specified to run when you shut down the guest operating system.

In order to execute these commands, you need to modify `/etc/vmware-tools/tools.conf`. The commands are:

`halt-command = <command>`

(where `<command>` is the command to execute when you shut down the guest operating system)

`reboot-command = <command>`

(where `<command>` is the command to execute when you restart the guest operating system)

Passing a String from the Host Operating System to the Guest Operating System

With GSX Server and knowledge of a scripting language like Perl or NetShell (in a Windows 2000 guest operating system), you can pass a string from your virtual machine's configuration file in the host operating system to the guest operating system when you use the configuration file to launch a virtual machine.

What you pass to the guest operating system is up to you. This should only be done if you have a good understanding of a scripting language and know how to modify system startup scripts.

There are two ways of passing strings to a virtual machine's guest operating system:

1. You can place a string in the virtual machine's configuration file by setting the string to the `machine.id` parameter.

   For example, you can set this string:
   `machine.id = "Hello World."`

2. You pass the string to the guest operating system from the command line when you launch the virtual machine. See example 1 below.

You could pass items like the Windows system ID (SID), a machine name or an IP address. Inside the guest operating system startup script, you have the guest service retrieve this string, which can then be used in another script you write and include in the startup script to set your virtual machine's system ID, machine name or IP address.

This way, you can make copies of the same configuration file, add a different string to each (either in the configuration file itself or at the command line), then use these variations of the same configuration file to launch the same virtual disk in nonpersistent mode multiple times in a training or testing environment, for example.

This is what portions of two configuration files that point to the same virtual disk might look like. Each configuration file contains its own unique string set for the `machine.id` parameter.

`<config_file_1>.vmx` contains:

```
ide0:0.present = TRUE
ide0:0.fileName = "my_common_virtual_hard_drive.vmdk"
machine.id = "the_string_for_my_first_vm"
```

`<config_file_2>.vmx` contains:

```
ide0:0.present = TRUE
ide0:0.fileName = "my_common_virtual_hard_drive.vmdk"
machine.id = "the_string_for_my_second_vm"
```

Passing a string is also useful in situations where you want to deploy virtual machines on a network using a common configuration file, while providing each machine with its own unique identity. In this case, you specify the string at the command line (you need to launch each virtual machine with the `vmware -s` command) when you launch each virtual machine using this configuration file. See example 1 below.

Each virtual machine disk file must be copied into its own directory if it shares its file name with another virtual machine disk file.

In the following example, we use a Windows host and guest to illustrate how you can use the guest service to retrieve a string containing what will become the virtual machine's machine name and IP address. We use W2K-VM as the machine name and 148.30.16.24 as the IP address.

1. Define a string. Do this by either:
   - Adding the following line to your virtual machine's configuration file:
     `machine.id = "W2K-VM 148.30.16.24"`
     then launching a virtual machine using this configuration file.
   - Launching a virtual machine from the command line. At the command line, type:
     ```
     C:\Program Files\VMware\Programs\vmware -s \
     'machine.id=W2K-VM 148.30.16.24' \
     C:\Documents and Settings\<username>\Local \
     Settings\My Documents\My Virtual \
     Machines\win2000\win2000.vmx
     ```
     Note: The above command must be written on one line with the backslashes ("\") at the end of each line removed.

     Note: On a Linux host, if a virtual machine ID is specified in a configuration file, and you use that file to launch a virtual machine, but you also specify a machine ID on the command line, the machine ID passed on the command line takes precedence and is passed to the guest operating system.
2. Retrieve the string in the virtual machine. In a Windows guest, the command to retrieve the string is
   `VMwareService --cmd machine.id.get`

   Note: In your Linux guest operating system's startup script, before the network startup section, add the following command:
   `/etc/vmware/vmware-guestd --cmd 'machine.id.get'`

You need to further customize this startup script so it uses the string the guest service retrieved during startup to set the virtual machine's network name to W2K-VM and its IP address to 148.30.16.24. This should be located in the script before the network services are started. If you're using a Windows 2000 guest operating system, for example, you can call the NetShell utility (`netsh`) and pass it the contents of the string, which then uses the string accordingly (that is, it can set a new IP address for the virtual machine, if that is what was passed in the string originally).

From your host operating system, you can prevent a string from being passed to the guest operating system via the guest service. To do this, set the following line in your virtual machine's configuration file.

```
isolation.tools.machine.id.get.disable = TRUE
```

Passing Information Between the Guest Operating System and a VMware Scripting API Script

When the guest operating system is running inside a virtual machine, the VMware guest operating system service allows you to pass information from a VMware Scripting API script you created (that is running in another host machine) to the guest operating system and from the guest operating system to a script.

For more information, visit the VMware Web site at *www.vmware.com/support/developer*.

6

Managing Virtual Machines

Managing Virtual Machines with VMware GSX Server

The following topics describe how to manage your virtual machines with GSX Server:

- Remotely Managing Virtual Machines on page 144
- Registering the Configuration Files for Virtual Machines on page 145
  - Registering a Virtual Machine on a Windows Host on page 146
  - Unregistering a Virtual Machine on a Windows Host on page 146
  - Registering a Virtual Machine on a Linux Host on page 147
  - Unregistering a Virtual Machine on a Linux Host on page 147
- Securing Your Virtual Machines on page 148
  - Understanding Permissions in a Running Virtual Machine on page 148
  - Authentication and Security Features on a Windows Host on page 149
  - Authentication and Security Features on a Linux Host on page 151
  - Checking Permissions in the VMware Management Interface on page 153
  - Securing Your Remote Sessions on page 153
- Identifying a Virtual Machine by Its UUID on page 158
  - Generating the UUID Automatically on page 158
  - Comparing the Generated UUID to Configuration File Parameters on page 159
  - Setting the UUID for a Virtual Machine that Is Not Being Moved on page 159
  - Setting the UUID for a Virtual Machine that Is Being Moved on page 159
- Using the VMware Management Interface on page 161
  - Setting the Session Length for the VMware Management Interface on page 163
  - Logging In to the VMware Management Interface on page 163
  - Using the Status Monitor on page 165
  - Viewing Details About a Virtual Machine on page 171
  - Downloading Remote Management Packages on page 175
  - Creating a New Virtual Machine from the Management Interface on page 177

- Deleting a Virtual Machine Using the VMware Management Interface on page 181
- Configuring the VMware GSX Server Host on page 182
- Logging Out of the VMware Management Interface on page 182
- The Apache Server and the Management Interface on page 183
- Setting a MIME Type to Launch the VMware Remote Console on page 183

Remotely Managing Virtual Machines

One of the primary strengths of GSX Server is the ability to manage your virtual machines remotely — that is, from any machine that can connect to your GSX Server host. You are not restricted to interacting with your virtual machines only on the host on which they are stored.

Remote management has many components and levels. For a high level view of your GSX Server host, use the VMware Management Interface, a Web-based tool for managing your virtual machines and the server host. For more information about the management interface, see Using the VMware Management Interface on page 161.

If you need to interact with a virtual machine directly from a remote location, for instance, if you need to maintain a database stored in a virtual machine, use the VMware Remote Console. The remote console displays your virtual machine in a window, and you interact with the virtual machine in this window as you would use a physical computer. For more information about remote consoles, see Using Local and Remote Consoles on page 185.

For a more automated way to remotely manage virtual machines and the GSX Server host, use the VMware Scripting APIs. If you are connecting to a GSX Server host from a Windows remote machine, you can use the VmCOM and VmPerl Scripting APIs. If you are connecting to a GSX Server host from a Linux remote machine, you can use the VmPerl Scripting API. For more information, visit the VMware Web site at *www.vmware.com/support/developer*.

Another automated way to manage virtual machines is to use the `vmware-cmd` utility. For more information, visit the VMware Web site at *www.vmware.com/support/developer*.

Finally, you can use third party tools to remotely manage your virtual machines. You can use applications like Windows Terminal Services or Windows XP Remote Desktop. Your site may use one of these tools as a standard method for remote access. In some situations, a remote access protocol can provide better performance over slow speed connections than the VMware Remote Console. However, the remote console is a better alternative on networks when you need to work intensively in the virtual machine's graphical user interface, as mouse responsiveness in a remote console session that is remotely displayed is slowed somewhat.

Registering the Configuration Files for Virtual Machines

GSX Server requires that each virtual machine's configuration file be registered before it can be accessed by VMware Remote Consoles and the VMware Management Interface. When you create a new configuration file with the New Virtual Machine Wizard (Windows hosts), Configuration Wizard (Linux hosts) or VMware Management Interface, whether for a new or an existing virtual machine, the configuration file is registered automatically with GSX Server.

When you register a virtual machine, you can easily connect to the virtual machine as the configuration file associated with the virtual machine appears in the VMware Management Interface, the **Virtual Machine Name** list in the local console (Windows hosts only) and the Connect to VMware Virtual Machine dialog box that appears when you connect to a virtual machine with the VMware Remote Console.

In the local console on a Windows host, a registered virtual machine appears in the **Virtual Machine Name** list with a hand icon ( ) while an unregistered virtual machine appears without the hand icon ( ).

If you are using a virtual machine created on another host machine, or that you migrated from another VMware product, you must register the configuration file by choosing one of the following procedures below. For more information about migrating virtual disks and virtual machines, see Moving and Sharing Virtual Machines on page 241.

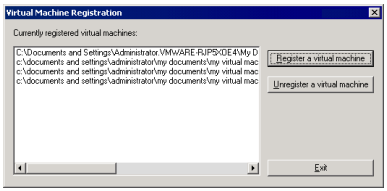
If you do not have a current need for a virtual machine, but do not want to delete it, you can unregister it instead. An unregistered virtual machine no longer appears in the VMware Management Interface.

Registering a Virtual Machine on a Windows Host

To register a virtual machine on a Windows host, do one of the following:

- If you are connected with a local console to the virtual machine you want to register, choose **File** > **Register this virtual machine**. Or, in the **Virtual Machine Name** list, right-click the virtual machine and choose **Register**.
- If you are not connected to the virtual machine you want to register, do the following:

  A. Choose **Start** > **Programs** > **VMware** > **Register a Virtual Machine**. The Virtual Machine Registration dialog box appears.


Virtual Machine Registration
Currently registered virtual machines:
C:\Documents and Settings\Administrator.VMWARE-RJPSXDE4\My D
c:\documents and settings\administrator\my documents\my virtual mac
c:\documents and settings\administrator\my documents\my virtual mac
c:\documents and settings\administrator\my documents\my virtual mac
Register a virtual machine
Unregister a virtual machine
Exit

  B. Click **Register a virtual machine**. A file selection dialog box appears.

  C. Select the configuration file for the virtual machine you want to register (it has a `.vmx` extension) and click **Open**. A message appears, telling you that the configuration file has been successfully registered.

  D. Click **Exit**. The Virtual Machine Registration dialog box closes.

Unregistering a Virtual Machine on a Windows Host

1. Choose **Start** > **Programs** > **VMware** > **Register a Virtual Machine**. The Virtual Machine Registration dialog box appears.
2. Select the virtual machine you want to unregister.
3. Click **Unregister a virtual machine**. The configuration file for this virtual machine no longer appears in the VMware Management Interface and the Connect to VMware Virtual Machine dialog box that appears when you connect to a virtual machine with a remote console. The virtual machine still may appear in the **Virtual Machine Name** list in the local console, provided you have accessed the virtual machine previously; it appears unregistered.

Registering a Virtual Machine on a Linux Host

To register a virtual machine, complete the following steps.

1. Decide which virtual machines you want to manage remotely that are not already registered.
2. Connect to the virtual machine in a local console.
   `vmware -G <path_to_config>.cfg`
3. Choose **File** > **Register this Virtual Machine**.

Default permissions are set on the configuration file. You are welcome to change these permissions to suit your needs.

Configuration files for virtual machines created with GSX Server on a Linux host have the following default permissions, based on the user accessing it:

- **Read**, **execute** and **write** - for the user who created the configuration file (the owner)
- **Read** and **execute** - for the group
- **Read** - for users other than the owner or a member of the owner's group

If you are importing a virtual machine **without** its configuration file from another VMware product, you need to create a new configuration file with the Configuration Wizard. When you first save the configuration file, it is automatically registered.

If you are importing a virtual machine **and** its configuration file from another VMware product, you need to register the configuration file in order to connect to the virtual machine from a console or the VMware Management Interface. Then you need to change the permissions on the configuration file to their default settings (that is, use `chmod 754 /<path_to_config>/<config>.cfg`). For more information about permissions, see Authentication and Security Features on a Linux Host on page 151.

Unregistering a Virtual Machine on a Linux Host

1. Connect to the virtual machine in a local console.
   `vmware -G <path_to_config>.cfg`
2. Choose **File** > **Unregister this Virtual Machine**.

Securing Your Virtual Machines

This section describes how you can set permissions and implement security features for your virtual machines and the server host.

Understanding Permissions in a Running Virtual Machine

Access to a virtual machine is based on the permissions granted to a user with regards to the virtual machine's configuration file (`.vmx` on a Windows host, `.cfg` on a Linux host). Different permissions give the user different types of access to a virtual machine.

In addition, the virtual machine must be registered before you can connect to it remotely. To register a virtual machine, see Registering the Configuration Files for Virtual Machines on page 145.

A virtual machine runs with the permissions of the user that connects to it. The first connected user necessarily has **Read & Execute** and **Write** permissions for a virtual machine on a Windows host, and read, write and execute (`r`, `w` and `x`) permissions for a virtual machine on a Linux host. The name of this user appears in the VMware Management Interface and in the Connected Users dialog box, which you access in the VMware Remote Console by choosing **Settings** > **Connected Users**.

If another user connects to the virtual machine with **Read** permission only, that user has the capabilities allowed by the **Read** permission; for instance, on a Windows host, the user cannot save changes to the virtual machine's configuration file or change the power state of the virtual machine (power it on or off, suspend, resume or reset it).

Since only one user can connect through the local console, only a user with **Read & Execute** and **Write** permissions can launch a virtual machine from a local console on a Windows host; only a user with read, write and execute (`r`, `w` and `x`) permissions can launch a virtual machine from a local console on a Linux host. No one else can connect to this virtual machine, regardless of his or her permissions.

When an administrator grants **Read & Execute** and **Write** permissions (Windows hosts) or **read**, **write** and **execute** (`r`, `w` and `x`) permissions (Linux hosts) to a user for a particular virtual machine, the administrator should make sure that the user has permission to access all of the files that the virtual machine uses while running, specifically the virtual disk (`.vmdk` file), `nvram` and log file.

One way to ensure this is to keep these files together in the same directory with the virtual machine's configuration file (when you configure a new virtual machine, all the files are created in the same directory) and assign permissions to all of the files at the same time.

Authentication and Security Features on a Windows Host

How GSX Server for Windows Authenticates Users

Every time a VMware Remote Console or VMware Management Interface makes a connection to the GSX Server host, the VMware Authorization Service requests a username and password, then authenticates only valid users. When connecting with a remote console, the service first checks to see if the user account is local, then if it is on the domain. This can have implications if the user connecting has the same user name locally and on the domain, but with different permissions, and the user intends to connect with the local account but passes an incorrect password. The user can connect to the virtual machine, but the power on may fail.

When connecting with the VMware Management Interface, the service only authenticates local user accounts.

Issues may also arise if a virtual machine is created by a local user but is modified by a user in the domain.

Once a user is authenticated, the VMware Authorization Service accepts a pathname to a virtual machine configuration file. If the virtual machine associated with the configuration file is not running, the service starts a new, separate process for the virtual machine as the user making the connection. A separate process is started for the remote console. If the virtual machine is already running as another process, the service connects you to that process and starts a new process for the remote console.

Note: If you are connecting to a virtual machine with the local console, the console and the virtual machine are the same process.

The VMware Authorization Service listens on port 902 for VMware Remote Console connections. For the VMware Management Interface, the service listens on ports 8222 and 8333 (for encrypted connections). For the local console, the service listens on the named pipe.

Access to the configuration file is restricted in the following ways:

On a Windows Server 2003 or Windows 2000 host, if a user has:

- All permissions for the configuration file denied, then the user cannot connect to the virtual machine at all. If a permission for a user is both allowed and denied, the denial takes precedence. If permissions are neither allowed nor denied, then the user is considered to have no permissions.
- **Read** permission for the configuration file, then the user can connect to the virtual machine only if the virtual machine is already running. The user cannot

power the virtual machine on or off, nor can the user reset, suspend or resume the virtual machine. The user cannot save changes to the configuration file.

- **Read & Execute** and **Write** permissions for the configuration file, then the user can connect to the virtual machine, whether it is running or not. The user can perform all of the virtual machine's power operations, such as powering on and off, resetting, suspending and resuming. The user can modify the configuration file.

On a Windows NT host, if a user has:

- **No Access** permission for the configuration file, then the user cannot connect to the virtual machine at all.
- **Read** permission for the configuration file, then the user can connect to the virtual machine only if the virtual machine is already running. The user cannot power the virtual machine on or off, nor can the user reset, suspend or resume the virtual machine. The user cannot save changes to the configuration file.
- **Read**, **Execute** and **Write** permissions for the configuration file, then the user can connect to the virtual machine, whether it is running or not. The user can perform all of the virtual machine's power operations, such as powering on and off, resetting, suspending and resuming. The user can modify the configuration file.

Note: If you intend to configure a virtual machine to use a raw disk, you need to be a member of the PowerUsers or Administrators group.

Configuring Permissions to Access a Virtual Machine

The system administrator (that is, the administrator responsible for setting up the host running GSX Server, not necessarily the Windows Administrator login) can set the access permissions on the configuration file using the following procedure. In general, you would want your GSX Server users to have **Read** permission to virtual machine configuration files; you can add any specific users that should have **Read & Execute** and **Write** permissions.

1. Locate the configuration file on the host system. Right-click the configuration file and select **Properties**. The Properties dialog box appears.
2. Click the **Security** tab, then do one of the following, depending upon which Windows host operating system you are running.

   Windows Server 2003 and Windows 2000 hosts:

   A. In the Properties dialog box, select each user or group and select the appropriate permission, typically **Read**. If the permissions are inherited, you

may need to uncheck **Allow inheritable permissions from parent to propagate to this object**.

B. To specify that a user or group that should not have access to the configuration file, either click **Remove** or check all permissions in the **Deny** column to deny all permissions to that user or group.

C. To add more users or groups, click **Add**. The Select Users, Computers and Groups dialog box appears. In the dialog box, select the groups or users that you want to access the virtual machine and click **Add**. After you finish adding the users or groups, click **OK**. The users and groups are added with default **Read** and **Write** permissions. In the Properties dialog box, change the type of access for the user or group to the configuration file; choose either **Read** or **Read & Execute** and **Write**. Click **OK** to set the permissions to the configuration file.

Windows NT hosts:

A. Click the **Permissions** button. The File Permissions dialog box appears.

B. In the File Permissions dialog box, select each user or group and select the appropriate permission, typically **Read**.

C. For any users or groups that should not have access to the virtual machine at all, select the user or group and click **Remove** or change the permission to **No Access**.

D. To add more users or groups, click **Add**. The Add Users and Groups dialog box appears. In the dialog box, select the groups that are allowed to access the virtual machine; to select individual users, click **Show Users**. As you select each user or group, specify the type of access for the user to the configuration file; choose from **No Access**, **Read**, or **Special Access** (and select **Read**, **Write** and **Execute**). Click **OK** twice to set the permissions to the configuration file.

Authentication and Security Features on a Linux Host

GSX Server for Linux uses Pluggable Authentication Modules (PAM) for user authentication in the VMware Remote Console and the VMware Management Interface. The default installation of GSX Server uses standard Linux `/etc/passwd` authentication, but can be configured to use LDAP, NIS, Kerberos or another distributed authentication mechanism.

How GSX Server for Linux Authenticates Users

Every time a connection is made to the server running GSX Server, the `inetd` or `xinetd` process runs an instance of the VMware authentication daemon (`vmware-authd`). The `vmware-authd` process requests a username and password, then hands them off to PAM, which performs the authentication.

Once a user is authenticated, `vmware-authd` accepts a pathname to a virtual machine configuration file. The `vmware-authd` process starts a virtual machine process as the owner of the configuration file, not as the user connecting to the virtual machine. However, the user is still restricted by his or her permissions on the configuration file.

Access to the configuration file is restricted in the following ways:

- The user must have **read** access to the configuration file to see the virtual machine in the VMware Management Interface and to view its details. The user cannot change the power state of the virtual machine and cannot connect to the virtual machine with a remote console.
- The user must have **read** and **execute** access to the configuration file to connect to and control (start, stop, reset, suspend or resume) a virtual machine in a local console (that is, to start GSX Server with `vmware -G`), remote console or with the management interface.
- The user must have **read**, **write** and **execute** access to the configuration file to change the configuration with the Configuration Editor. This includes connecting and disconnecting devices.

Note: Even if you have full permissions on a configuration file, but you do not have **execute** permission to the directory in which the configuration file resides or any of its parent directories, then you cannot connect to the virtual machine with a VMware Remote Console or a VMware Scripting API. Further, you cannot see the virtual machine in the VMware Management Interface or in the Connect to VMware Virtual Machine dialog box when you connect to the GSX Server host with a VMware Remote Console. Nor can you delete any files in the virtual machine's directory.

If a `vmware` process is not running for this configuration file, `vmware-authd` checks to see if you registered this virtual machine. If the virtual machine is registered, `vmware-authd` becomes the owner of the configuration file (not necessarily the user that is currently authenticated) and starts GSX Server with this configuration file as an argument (for example,
`vmware /<path_to_config>/<configfile>.cfg`).

The `vmware-authd` process exits as soon as a connection is established to a `vmware` process and at least one used has connected. Each `vmware` process shuts down automatically after the last user disconnects.

Default Permissions

When you create a virtual machine with GSX Server, its configuration file is registered with the following default permissions, based on the user accessing it:

- **Read**, **execute** and **write** (7) — for the user who created the configuration file (the owner)
- **Read** and **execute** (5) — for the group
- **Read** (4) — for users other than the owner or a member of the owner's group

When you first install your GSX Server software and run the configuration program (`vmware-config.pl`), you can set these permissions for any existing configuration files for registered virtual machines. If you plan to use a virtual machine and its configuration file you created in other VMware products with GSX Server, you must register the configuration file in order to connect to the virtual machine from a console or the VMware Management Interface, then set the default permissions as above. For more information about registering configuration files, see Registering the Configuration Files for Virtual Machines on page 145.

Checking Permissions in the VMware Management Interface

The VMware Management Interface lists the permissions you have for each configuration file on the host machine to which you are connected. The permissions appear on the Users and Events page for each virtual machine.

Only registered virtual machines for which you have **read** access are visible to you in the VMware Management Interface.

Securing Your Remote Sessions

The username, password and network packets sent to the GSX Server host over a network connection when using the VMware Remote Console or the VMware Management Interface are not encrypted in GSX Server by default. As the Administrator user (Windows hosts) or root user (Linux hosts), you can enable Secure Sockets Layer (SSL) to encrypt these sessions.

When you enable SSL, security certificates are created by GSX Server and stored on your host. However, the certificates used to secure your VMware Management Interface sessions are not signed by a trusted certificate authority; therefore they do not provide authentication. If you intend to use encrypted remote connections

externally, you should consider purchasing a certificate from a trusted certificate authority.

Caution: GSX Server does not generate the security certificate for the VMware Management Interface on Windows NT 4.0 hosts. See Enabling SSL for the VMware Management Interface on a Windows NT Host on page 156.

With SSL enabled, the remote console and management interface perform exactly as they would if SSL were disabled.

When SSL is enabled for the VMware Remote Console, a lock icon appears in the lower right corner of the console window. Any remote consoles that are already open at the time SSL is enabled do not become encrypted, and the lock icon does not appear in these console windows. These consoles must be closed and new console sessions must be started to ensure encryption.

When SSL is enabled for the VMware Management Interface, the URL to connect to the management interface is `https://<hostname>:8333`. The management interface automatically redirects users to this URL if they use the original URL (`http://<hostname>:8222`) to connect. In addition, a lock icon appears in the status bar of the browser window.

Note: After SSL is enabled on a Windows host, any new management interface connections to the non-secure port (8222) are not redirected.

Note: If you disable SSL, users are automatically redirected to `http://<hostname>:8222` if they use `https://<hostname>:8333` to connect to the management interface.

Using Your Own Security Certificates

If you prefer, you can use your own security certificate when you enable SSL.

On a Windows host, run the Microsoft Management Console (`mmc.exe`) and select your certificate. When you upgrade the VMware Management Interface on a GSX Server for Windows host, you need to reassign your certificate to the management interface.

On a Linux host, the VMware Management Interface certificate must be placed in `/etc/vmware-mui/ssl`. The management interface certificate consists of 2 files: the certificate itself (`mui.crt`) and the private key file (`mui.key`). The private key file should be readable only by the root user.

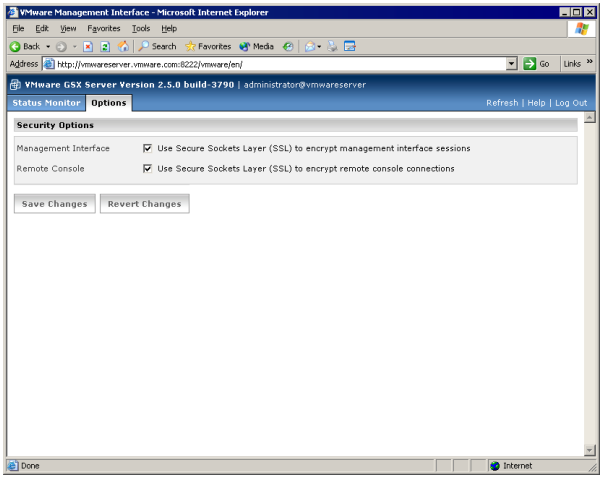
When you upgrade the VMware Management Interface on a Linux host, the certificate remains in place and, in case you removed the management interface, the directory is not removed from your host.

Enabling SSL for Remote Sessions

You enable SSL in the VMware Management Interface.

Remember that the certificates used in these secure sessions are not signed by a trusted certificate authority; therefore they do not provide authentication. If you intend to use encrypted remote connections externally, you should consider purchasing a certificate from a trusted certificate authority.

1. Log in to the VMware Management Interface as the Administrator (GSX Server for Windows hosts) or root user (GSX Server for Linux hosts).
2. On the Status Monitor page, click the **Options** tab. The Options page appears.



3. To secure your management interface sessions, check the **Use Secure Sockets Layer (SSL) to encrypt management interface sessions** check box.
4. To secure your remote console connections, check the **Use Secure Sockets Layer (SSL) to encrypt remote console connections** check box.
5. To save your settings, click **Save Changes**. After the changes are saved, a lock icon appears in the status bar of the browser running the VMware Management Interface. You need to accept the certificate in your browser. The lock icon appears in the status bar of any new VMware Remote Console window.

Enabling SSL for the VMware Management Interface on a Windows NT Host

In order to enable SSL for the VMware Management Interface on a Windows NT host, you must first generate a security certificate. Use Microsoft's Certificate Server to create a certificate in order to secure the management interface with SSL. To create the certificate on a Windows NT host, complete the following steps.

1. Download the Windows NT 4.0 Option Pack. You can find it at *www.microsoft.com/msdownload/ntoptionpack/askwiz.asp*.
2. Install the option pack.

   Caution: Make sure you install the Certificate Server when you install the option pack.
3. After the installation completes, open the Services window in the Windows Control Panel (choose **Start** > **Settings** > **Control Panel** > **Services**) and make sure the Certificate Authority (the name of the Certificate Server service) is running. If it is not running, select the service and click **Start**.
4. Create the management interface certificate. Choose **Start** > **Programs** > **Windows NT 4.0 Option Pack** > **Microsoft Internet Information Server** > **Internet Service Manager**.
5. Expand the Internet Information Server tree, then expand the tree for the GSX Server host machine name, then right-click the VMware Management Interface Web site and select **Properties**.
6. On the **Directory Security** tab, under **Secure Communications**, click **Key Manager**.
7. Select **WWW**, then choose **Key** > **Create New Key**.
8. Follow the wizard. Make sure you select **Automatically send the request to an online authority** and choose the **Microsoft Certificate Server** option.
9. When you are prompted to select the Web server bindings for this key, do one of the following:
   - If your GSX Server host has only one IP address, select **All unassigned** for the IP address and enter port 8333.
   - If your GSX Server host has multiple IP addresses, enter the correct IP address and port (8333) for this certificate.
10. After the wizard closes, choose **Computers** > **Exit** to return to the **Secure Communications** dialog box.
11. Check **Require Secure Channel when accessing this resource** and click **OK** to return to the **Directory Security** tab. Click **OK** to close the Properties dialog box,

then choose **Console** > **Exit** to close the Microsoft Management Console. Make sure you save your changes when you exit.

SSL is enabled for your management interface connections.

To disable SSL for your management interface connections, go to the Microsoft Management Console and uncheck **Require Secure Channel when accessing this resource** in the Secure Communications dialog box.

You do not need to create a certificate for the remote console manually on a Windows NT 4.0 host.

Identifying a Virtual Machine by Its UUID

Each GSX Server virtual machine is automatically assigned a universally unique identifier (UUID), which is stored in the SMBIOS system information descriptor. It can be accessed by standard SMBIOS scanning software — for example SiSoftware Sandra or the IBM utility `smbios2` — and used for systems management in the same ways you use the UUID of a physical computer.

The UUID is a 128-bit integer. The 16 bytes of this value are separated by spaces except for a dash between the eighth and ninth hexadecimal pairs. So a sample UUID might look like this:

```
00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff
```

Generating the UUID Automatically

The automatically generated UUID is based on the physical computer's identifier and the path to the virtual machine's configuration file. This UUID is generated when you power on or reset the virtual machine. The UUID that is generated remains the same so long as the virtual machine is not moved or copied.

The automatically generated UUID is also written to the virtual machine's configuration file as the value of `uuid.location`.

If you move or copy the virtual machine, a new UUID is generated when the virtual machine is powered on — based on the physical computer's identifier and path to the virtual machine's configuration file in its new location.

If you suspend and resume a virtual machine, this does not trigger the process that generates a UUID. Thus, the UUID in use at the time the virtual machine was suspended remains in use when the virtual machine is resumed, even if it has been copied or moved. However, the next time the virtual machine is rebooted, the UUID is generated again. If the virtual machine has been copied or moved, the UUID is changed.

In some circumstances — for example, if you are moving the virtual machine but want to keep the same UUID — you may want to assign a specific UUID to the virtual machine. In that case, you need to override the automatically generated UUID value. To do so, edit the virtual machine's configuration file as described in this section to set the value of the parameter `uuid.bios`.

Comparing the Generated UUID to Configuration File Parameters

When a virtual machine is powered on or reset, GSX Server generates a UUID as described above and compares it to the values for `uuid.location` and (if it exists) `uuid.bios` in the configuration file.

If the automatically generated UUID matches the value of `uuid.location`, GSX Server checks for `uuid.bios`. If `uuid.bios` exists, its value is used as the virtual machine's UUID. If `uuid.bios` does not exist, the automatically generated value is used.

If the automatically generated UUID does not match the value of `uuid.location`, the newly generated value is used as the virtual machine's UUID and is saved to the configuration file, replacing the previous value of `uuid.location` and (if it exists) `uuid.bios`.

Note: Any changes to the UUID take effect only after the virtual machine is rebooted.

Setting the UUID for a Virtual Machine that Is Not Being Moved

To assign a specific UUID to a virtual machine that is not being moved, add one line to the configuration file. You need to use a text editor to edit the configuration file, located in your virtual machine's directory; the file has a `.vmx` extension on a Windows host and a `.cfg` extension on a Linux host. The format for the line is:

```
uuid.bios = <uuidvalue>
```

The UUID value must be surrounded by quotation marks. A sample configuration line might look like this:

```
uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"
```

After adding this line to the configuration file, restart the virtual machine. The new UUID is used when the virtual machine restarts.

Setting the UUID for a Virtual Machine that Is Being Moved

If you plan to move a virtual machine and want it to have the same UUID it did before the move, you must note the UUID being used before the move and add that UUID to the configuration file after the move. Follow these steps:

1. Before moving the virtual machine, examine its configuration file. You need to use a text editor. The configuration file is located in your virtual machine's directory; the file has a `.vmx` extension on a Windows host and a `.cfg` extension on a Linux host.

If the virtual machine's UUID has been set to a specific value, the configuration file has a line that begins with `uuid.bios`. Note the 128-bit hexadecimal value that follows. This is the value you should use in the new location.

If there is no line beginning with `uuid.bios`, look for the line that begins with `uuid.location` and note the 128-bit hexadecimal value that follows it.

2. Move the virtual machine's files to the new location. For more information, see Moving a Virtual Machine to a New Host Machine on page 245.
3. Start the virtual machine, then shut it down.
4. Edit the virtual machine's configuration file to add a `uuid.bios` line, as described in Setting the UUID for a Virtual Machine that Is Not Being Moved on page 159. Set the value of `uuid.bios` to the value you recorded in step 1.
5. Start the virtual machine. It should now have the same UUID as it did before the move.

Using the VMware Management Interface

GSX Server provides the VMware Management Interface, a Web-based management tool that allows you to

- Monitor the state of virtual machines and the GSX Server host on which they are running.
- Control (power on, suspend, resume, reset and power off) the virtual machines on that host.
- Connect the VMware Remote Console to a given virtual machine, for hands-on management.
- View details about each virtual machine, including system summary, hardware information, any connected users and a log of recent events.
- Create and delete virtual machines.
- Secure remote console and management interface sessions with SSL.
- Answer questions and acknowledge messages posed by the virtual machine.

To use the VMware Management Interface, make sure you set **read** permissions for all users for each virtual machine you want to manage from a browser when you register each virtual machine. Read more about security and GSX Server on Securing Your Virtual Machines on page 148.

To properly view the VMware Management Interface, you should ensure that style sheets are enabled in your browser, regardless of which browser and version you are using.

Note: If you intend to run the VMware Management Interface in Internet Explorer 6.0 on a Windows Server 2003 system, whether the GSX Server host installed on Windows Server 2003 or a Windows Server 2003 client machine that connects to a GSX Server host, there are some special configuration steps needed in order to use the management interface. For more information, see Configuring Internet Explorer 6.0 to Use the VMware Management Interface on page 61.

Note: You can only use ASCII characters when viewing the management interface.

The VMware Management Interface starts with a Login page. The Login page contains a download menu where you can download the VMware Remote Console for Windows and Linux hosts. This menu can be customized to suit your users' needs, for instance, if you want users to be able to install the VMware Scripting APIs on their

remote clients. You can add more files to the download menu, hide items already listed and even hide the link or the menu itself. For more information, see Downloading Remote Management Packages on page 175.

Once your user name and password are authorized by the management interface, the Status Monitor page appears. The Status Monitor page contains high level details about all the virtual machines on the host server to which you are connected. The Status Monitor page links to a detailed set of pages specific to each virtual machine, where you find information about virtual devices, configuration options and a summary of recent events. In addition, you can create and delete virtual machines from your browser.

These pages refresh or reload automatically; refreshing every 90 seconds. You may want to refresh or reload these pages manually before you perform an operation like suspending, resuming, or powering on or off a virtual machine from the management interface — or after you perform a power operation in a remote console — in case another user has performed the same or a conflicting operation right before you. To refresh the page, click **Refresh** at the top of a page.

This section includes the following topics:

- Setting the Session Length for the VMware Management Interface on page 163
- Logging In to the VMware Management Interface on page 163
- Using the Status Monitor on page 165
- Viewing Details About a Virtual Machine on page 171
- Downloading Remote Management Packages on page 175
- Creating a New Virtual Machine from the Management Interface on page 177
- Deleting a Virtual Machine Using the VMware Management Interface on page 181
- Configuring the VMware GSX Server Host on page 182
- Logging Out of the VMware Management Interface on page 182
- Setting a MIME Type to Launch the VMware Remote Console on page 183
- The Apache Server and the Management Interface on page 183

Setting the Session Length for the VMware Management Interface

Your management interface sessions times out after a 60 minute period of idle time.

This setting is specified by the variable `vmware_SESSION_LENGTH`, stored in `C:\Program Files\VMware\VMware Management Interface\htdocs\init.pl` (on a Windows host) or `/home/vmware/mui/apache/conf/access.conf` (on a Linux host). You can change this setting to any number of minutes, or you block access to the management interface for all users by setting `vmware_SESSION_LENGTH` to 0 minutes. In addition, you can allow for persistent sessions that never time out by setting `vmware_SESSION_LENGTH` to `-1`.

Logging In to the VMware Management Interface

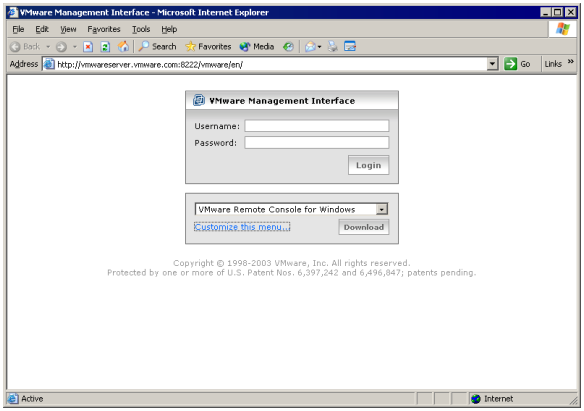
To use the VMware Management Interface, you should be running Internet Explorer 5.5 or 6.0 (VMware highly recommends using 6.0), Netscape Navigator 7.0 or Mozilla 1.x. You need to know the host name or IP address of the server you want to manage. You must have a valid user name and password on that server.

The URL to connect to the server is `http://<hostname>:8222`.

Note: If you are connecting to the management interface from a browser on the host machine, you can use `localhost` as the `<hostname>`.

Note: If your management interface sessions are encrypted with SSL, the URL to connect to the server is `https://<hostname>:8333`. For more information, see Securing Your Remote Sessions on page 153.

Enter the URL. The Login page appears.



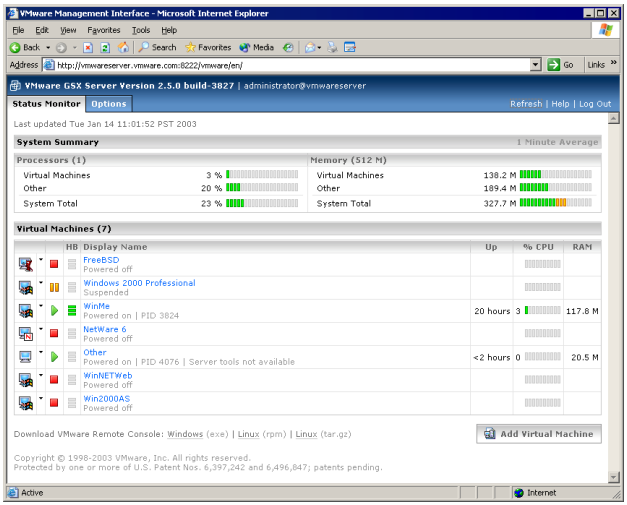
The Login page contains fields for your user name and password.

It also contains a download menu from which you can download installation packages for the VMware Remote Console. To download a package, see Downloading Remote Management Packages on page 175.

On the Login page, enter your user name and password for the host machine, then click **Login**. The Status Monitor page appears.

Using the Status Monitor

The Status Monitor page contains a high-level view of the GSX Server host including a host system summary and list of all registered virtual machines.



Viewing Summary Information about the GSX Server Host System

Under **System Summary**, while at least one virtual machine is powered on, you can view:

- The number of processors on the GSX Server host, including the average percentage of CPU usage used by virtual machines, other processes on the host and the total being used by the whole system for the previous minute.
- The amount of memory on the GSX Server host, including the average amount of memory used by virtual machines, other processes on the host and the total being used by the whole system for the previous minute.

Viewing Summary Information about Virtual Machines on the Host

Under **Virtual Machines**, you can view a list of all registered virtual machines on the host. Activities you can perform include:

- Connecting to a Virtual Machine with the VMware Remote Console on page 166
- Using the Virtual Machine Menu on page 167
- Changing the Power State of a Virtual Machine on page 168
- Monitoring the Virtual Machine's Heartbeat on page 168

- Viewing Information about a Virtual Machine on page 169
- Downloading Remote Management Packages on page 175 (Login and Status Monitor pages)
- Creating a New Virtual Machine on page 169 (Status Monitor page only)
- Deleting a Virtual Machine on page 169
- Configuring the GSX Server Host on page 170 (Options page only)
- Using Common Controls on page 170

Connecting to a Virtual Machine with the VMware Remote Console

If you need to view a particular virtual machine's desktop, you can attach the VMware Remote Console and connect to the virtual machine. Click the terminal icon ( ) to launch the remote console. For more information on connecting the remote console, see Starting the Remote Console on a Windows Remote Workstation on page 189 and Starting the Remote Console on a Linux Remote Workstation on page 190.

Note: If you are connecting a version 2.0 remote console to a version 2.5 server, you need to select the virtual machine after you connect to the server host. VMware recommends you update the remote console on this client. Download the appropriate installer on the Status Monitor page. See Downloading Remote Management Packages on page 175.

Netscape and Mozilla users must define a MIME type for the console first; Internet Explorer is automatically configured when the remote console is installed. For more information, see Setting a MIME Type to Launch the VMware Remote Console on page 183.

The terminal icon appears slightly differently, depending upon the guest operating system installed in the virtual machine. This visual cue helps to identify the virtual machine, for example, when the display name does not indicate the guest operating system. Below are the different ways the terminal icon appears in the management interface.

— indicates a Windows guest operating system.

— indicates a Linux guest operating system.

— indicates a FreeBSD guest operating system.

— indicates a NetWare guest operating system.

— indicates other guest operating systems.

Using the Virtual Machine Menu

Click the arrow to the right of the terminal icon ( ) to display a menu of options for the virtual machine. The menu includes the following commands, most of which can be performed using the buttons and other visual elements of the management interface. Depending on your permissions and the state of the virtual machine, some options may not be available.

- **Attach Remote Console** — launches the VMware Remote Console, which connects to this virtual machine. This is the same as clicking . You need to log in to the host. For more information, see Connecting to Virtual Machines from Local and Remote Consoles on page 187.

  Note: Netscape and Mozilla users must define a MIME type for the console first; Internet Explorer is automatically configured when the remote console is installed. For information, see Setting a MIME Type to Launch the VMware Remote Console on page 183.
- **Properties** — opens the Virtual Machine Overview page for this virtual machine in a new browser window. This is the same as clicking the display name link in the **Display Name** column.
- **Shut Down Guest** — shuts down the guest operating system, powers off the virtual machine then runs the script associated with this power state change. This is the same as clicking in the power state popup.
- **Suspend after Running Script** — runs the associated script then suspends a running virtual machine. This is the same as clicking in the power state popup.
- **Power On/Resume and Run Script** — powers on a stopped virtual machine or resumes a suspended virtual machine, then runs the script associated with this power state change. This is the same as clicking in the power state popup.
- **Restart Guest** — restarts the guest operating system and the virtual machine. This is the same as clicking in the power state popup.
- **Power Off** — powers off the virtual machine immediately without running a script. This is the same as turning off the power to a physical computer.
- **Suspend** — suspends a powered on virtual machine without running a script.
- **Power On/Resume** — powers on a stopped virtual machine or resumes a suspended virtual machine without running a script.
- **Reset** — resets the virtual machine immediately without running a script. This is the same as pressing the reset button on a physical computer.

- **Delete Virtual Machine** — lets you delete a virtual machine or just its configuration, provided the virtual machine is powered off. See Deleting a Virtual Machine Using the VMware Management Interface on page 181.

Changing the Power State of a Virtual Machine

Depending upon your permissions, you can change the power state of the virtual machine in the management interface. Your permissions are listed in the **Users and Events** tab for the virtual machine. For more information, see Viewing a List of Connected Users on page 173.

To change the virtual machine's power state, click the button that indicates the virtual machine's current power state. A popup menu appears, displaying the following buttons:

Button	Description
	Shuts down the guest operating system and powers off the virtual machine. GSX Server closes any open applications and shuts down the guest operating system before powering off the virtual machine. VMware Tools executes the script associated with this power state change, if any. When this icon is red, the virtual machine is powered off.
	Suspends a running virtual machine or resumes a suspended virtual machine. VMware Tools executes the script associated with this power state change, if any. When this icon is amber, the virtual machine is suspended.
	Powers on a stopped virtual machine or resumes a suspended virtual machine. VMware Tools executes the script associated with this power state change, if any. When this icon is green, the virtual machine is running.
	Restarts a guest operating system. GSX Server closes any open applications and shuts down the guest operating system before restarting the guest operating system.

Changing the power state executes any script associated with the power state change. For more information about running scripts, see Executing Scripts When the Virtual Machine's Power State Changes on page 122.

Monitoring the Virtual Machine's Heartbeat

Under **HB** is a bar graph that represents the percentage of the number of heartbeats actually sent by the VMware guest operating system service to the virtual machine from its guest operating system, relative to the number of heartbeats the virtual machine expects to receive, for the minute before the page was last updated. Heavily loaded guest operating systems may not send 100% of the expected heartbeats, even though the system is otherwise operating normally; in general, only when the

heartbeat percentage drops to zero should the virtual machine or guest operating system be considered abnormal.

Note: If VMware Tools is not installed or is not running, the guest operating system does not send any heartbeats to its virtual machine and this meter is disabled.

Viewing Information about a Virtual Machine

Important virtual machine information is readily available on the Status Monitor page.

- The link in the **Display Name** column indicates the display name for the virtual machine; if one is not specified, then the path to the configuration file for the virtual machine appears here instead. This column also contains the virtual machine's power state and its process ID (if it is running); it notes if VMware Tools is not installed and, if a local console is attached to the virtual machine, that remote management prohibited.

  If the virtual machine is waiting for a response to a system message, a "Waiting for input" link appears here. Click the link to view the message and respond to it.

  Click the virtual machine link for more details about the virtual machine. The Virtual Machine Overview page appears in a new browser window. For more information, see Viewing Details About a Virtual Machine on page 171.
- The value in the **Up** column indicates the length of time the virtual machine has been running.
- The value in the **% CPU** column indicates the average percentage of host operating system processor capacity the virtual machine used during the final minute before the page was last updated. More detailed processor information is available on the Virtual Machine Overview page.
- The value in the **RAM** column indicates the average amount of memory the virtual machine used during the final minute before the page was last updated. More detailed memory information is available on the Virtual Machine Overview page.

Creating a New Virtual Machine

To create a new virtual machine from the management interface, on the Status Monitor page, click **Add Virtual Machine**. The Add Virtual Machine page appears. For information on creating a virtual machine from the management interface, see Creating a New Virtual Machine from the Management Interface on page 177.

Deleting a Virtual Machine

To delete a virtual machine from the management interface, click the arrow to the right of the terminal icon ( ) and choose **Delete Virtual Machine**. The Confirm:

Deleting <Virtual Machine> page appears in a new window. For information on deleting a virtual machine from the management interface, see Deleting a Virtual Machine Using the VMware Management Interface on page 181.

Configuring the GSX Server Host

The **Options** tab lets you make changes to your GSX Server configuration on the host. For more information, see Configuring the VMware GSX Server Host on page 182.

Note: Only a user with administrator privileges (Windows hosts) or the root user (Linux hosts) can access this tab.

Common Controls

In addition, the following links appear on most or all of the pages in the management interface.

Refresh — This link refreshes or reloads the current page. To avoid conflicts with other users, click this button before you perform an operation in the management interface like shutting down, suspending, resuming or powering on a virtual machine — or **after** you perform such an operation in a remote console.

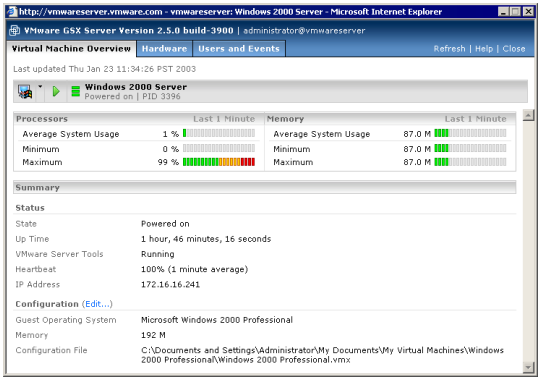
Help — This link connects you to the GSX Server online documentation for the current page in the management interface.

Logout — This link logs you out of the management interface. You can only log out from the Status Monitor and Options pages. Click **Logout** to return to the Login page. See Logging Out of the VMware Management Interface on page 182.

Close — Closes the current management interface window. You can only close windows on the Add Virtual Machine, Virtual Machine Overview, Hardware and Users and Events pages.

Viewing Details About a Virtual Machine

To see more information about a particular virtual machine, click the link to that virtual machine in the **Display Name** column on the Status Monitor page. The Virtual Machine Overview page appears in a new browser window.


http://vmwareserver.vmware.com - vmwareserver: Windows 2000 Server - Microsoft Internet Explorer
VMware GSX Server Version 2.5.0 build-3900 | administrator@vmwareserver
Virtual Machine Overview
Hardware
Users and Events
Refresh | Help | Close
Last updated Thu Jan 23 11:34:26 PST 2003
Windows 2000 Server
Powered on | PID 3396
Processors
Last 1 Minute
Average System Usage 1 %
Minimum 0 %
Maximum 99 %
Memory
Last 1 Minute
Average System Usage 87.0 M
Minimum 87.0 M
Maximum 87.0 M
Summary
Status
State Powered on
Up Time 1 hour, 46 minutes, 16 seconds
VMware Server Tools Running
Heartbeat 100% (1 minute average)
IP Address 172.16.16.241
Configuration (Edit...)
Guest Operating System Microsoft Windows 2000 Professional
Memory 192 M
Configuration File C:\Documents and Settings\Administrator\My Documents\My Virtual Machines\Windows 2000 Professional\Windows 2000 Professional.vmx

The Virtual Machine Overview page contains the following information:

- The current power state of the virtual machine — whether it is powered on, powered off or suspended.
- The process ID of the virtual machine.
- The minimum, maximum and average percentage of host operating system processor capacity that the virtual machine used in the previous minute.
- The minimum, maximum and average amount of host operating system memory that the virtual machine used in the previous minute.
- How long the virtual machine has been running.
- VMware Tools status; whether VMware Tools is installed and running.
- The average percentage of heartbeats received by a virtual machine during the previous minute. See Using the Status Monitor on page 165.
- The IP address of the virtual machine.
- A link to edit the virtual machine's configuration. Click **Edit**. A VMware Remote Console launches, connecting to the virtual machine. In the console, choose **Settings** > **Configuration Editor** to modify the virtual machine's configuration.
- The guest operating system installed in the virtual machine.
- The amount of memory allocated to the virtual machine.

- The path to the virtual machine's configuration file on the GSX Server host.

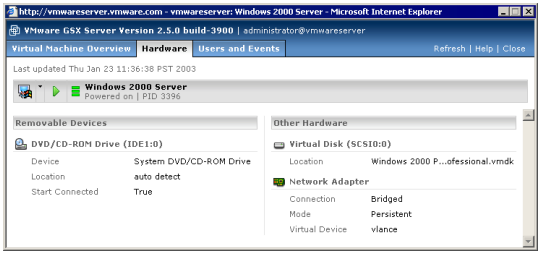
Activities you can perform when viewing a virtual machine's details include:

- Connecting to a Virtual Machine with the VMware Remote Console on page 166
- Using the Virtual Machine Menu on page 167
- Changing the Power State of a Virtual Machine on page 168
- Using Common Controls on page 170
- Viewing a Virtual Machine's Hardware on page 172
- Viewing a List of Connected Users on page 173
- Viewing a Log of a Virtual Machine's Events on page 174

Viewing a Virtual Machine's Hardware

To review the virtual hardware inside a virtual machine, click the **Hardware** tab. The Hardware page appears.

The Hardware page lists the virtual hardware in the virtual machine — configured devices like the virtual disk, CD-ROM or DVD-ROM drives and virtual network adapter. More information about each device is listed.



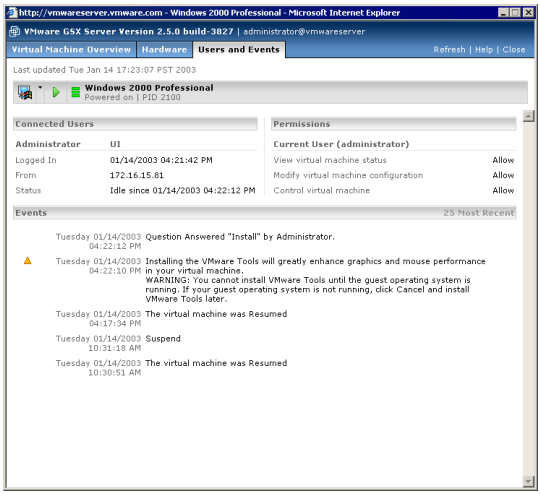
Activities you can perform when viewing a virtual machine's hardware include:

- Connecting to a Virtual Machine with the VMware Remote Console on page 166
- Using the Virtual Machine Menu on page 167
- Changing the Power State of a Virtual Machine on page 168
- Using Common Controls on page 170

Click the tabs at the top of the page to view the Virtual Machine Overview and Users and Events pages.

Viewing a List of Connected Users

To see a list of users that are connected to a virtual machine with a console or VMware Scripting API, click the **Users and Events** tab.


http://vmwareserver.vmware.com - Windows 2000 Professional - Microsoft Internet Explorer
VMware GSX Server Version 2.5.0 build-3827 | administrator@vmwareserver
Virtual Machine Overview
Hardware
Users and Events
Refresh | Help | Close
Last updated Tue Jan 14 17:23:07 PST 2003
Windows 2000 Professional
Powered on | PID 2100
Connected Users
Administrator
UI
Logged In
01/14/2003 04:21:42 PM
From
172.16.15.81
Status
Idle since 01/14/2003 04:22:12 PM
Permissions
Current User (administrator)
View virtual machine status
Allow
Modify virtual machine configuration
Allow
Control virtual machine
Allow
Events
25 Most Recent
Tuesday 01/14/2003 04:22:12 PM
Question Answered "Install" by Administrator.
Tuesday 01/14/2003 04:22:10 PM
Installing the VMware Tools will greatly enhance graphics and mouse performance in your virtual machine.
WARNING: You cannot install VMware Tools until the guest operating system is running. If your guest operating system is not running, click Cancel and install VMware Tools later.
Tuesday 01/14/2003 04:17:34 PM
The virtual machine was Resumed
Tuesday 01/14/2003 10:31:18 AM
Suspend
Tuesday 01/14/2003 10:30:51 AM
The virtual machine was Resumed

The list under **Connected Users** identifies any users connected to the virtual machine with a console or VMware Scripting API. The list includes when and from where the user connected to the virtual machine and the status of the user's activity.

The list under **Permissions** indicates what you can do with the virtual machine. You are either allowed or denied the following abilities:

- Viewing virtual machine status.
- Modifying the virtual machine's configuration.
- Controlling the virtual machine: powering it on or off, suspending or resuming it.

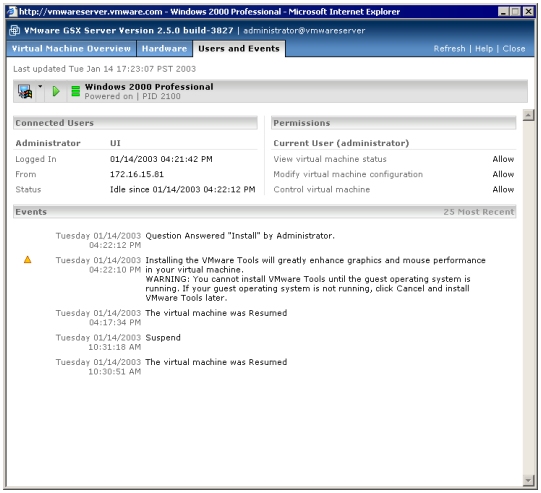
Activities you can perform when viewing a virtual machine's user and event information include:

- Connecting to a Virtual Machine with the VMware Remote Console on page 166
- Using the Virtual Machine Menu on page 167
- Changing the Power State of a Virtual Machine on page 168
- Using Common Controls on page 170

Click the tabs at the top of the page to view the Virtual Machine Overview and Hardware pages.

Viewing a Log of a Virtual Machine's Events

A log of the 25 most recent virtual machine events is available. Click the **Users and Events** tab. The Users and Events page appears.


http://vmwareserver.vmware.com - Windows 2000 Professional - Microsoft Internet Explorer
VMware GSX Server Version 2.5.0 build-3827 | administrator@vmwareserver
Virtual Machine Overview
Hardware
Users and Events
Refresh | Help | Close
Last updated Tue Jan 14 17:23:07 PST 2003
Windows 2000 Professional
Powered on | PID 2100
Connected Users
Administrator
UI
Logged In
01/14/2003 04:21:42 PM
From
172.16.15.81
Status
Idle since 01/14/2003 04:22:12 PM
Permissions
Current User (administrator)
View virtual machine status
Allow
Modify virtual machine configuration
Allow
Control virtual machine
Allow
Events
25 Most Recent
Tuesday 01/14/2003 04:22:12 PM
Question Answered "Install" by Administrator.
Tuesday 01/14/2003 04:22:10 PM
Installing the VMware Tools will greatly enhance graphics and mouse performance in your virtual machine.
WARNING: You cannot install VMware Tools until the guest operating system is running. If your guest operating system is not running, click Cancel and install VMware Tools later.
Tuesday 01/14/2003 04:17:34 PM
The virtual machine was Resumed
Tuesday 01/14/2003 10:31:18 AM
Suspend
Tuesday 01/14/2003 10:30:51 AM
The virtual machine was Resumed

The **Events** list displays a log of the most recent actions or events recorded in the virtual machine, such as the questions GSX Server asks, errors and other events like the powering on or off of the virtual machine. The events appear in reverse chronological order.

The event log draws its data from the log file for the virtual machine's configuration file stored, by default, in the virtual machine's folder. On a Windows Server 2003 or Windows 2000 host, this folder is `C:\Documents and Settings\<username>\Local Settings\My Documents\My Virtual Machines`. On a Windows NT host, this folder is `C:\WINNT\Profiles\<username>\Personal\My Virtual Machines\<guestOS>`. On a Linux host, this directory is `<homedir>/vmware/<guestOS>`.

When you perform an action within the management interface that prompts the virtual machine to generate a message needing your response before it can proceed, a waiting for input message appears in the **Display Name** column. When you click that link, a popup window appears, prompting you for a response. After you provide your answer, the popup window closes.

The log shows the date and time the event occurred and an explanation of the event. Some events have a symbol associated with them that corresponds to the type of event that occurred.

⚠ - This type of event indicates a question or a warning was generated by the virtual machine.

● - This type of event indicates an error occurred in the virtual machine.

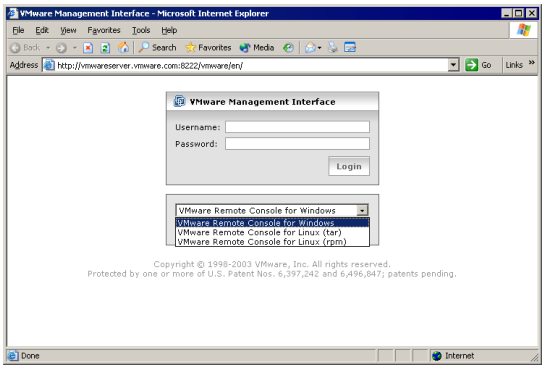
Click the tabs at the top of the page to view the Virtual Machine Overview and Hardware pages.

Note: On Windows hosts, the host operating system's own Event Log tracks virtual machine power state changes, GSX Server messages and answers to prompts that appear in the virtual machine.

Downloading Remote Management Packages

From the management interface, you can download installation packages for the VMware Remote Console. Packages are available for Linux and Windows hosts; download the package appropriate to the host machine on which it is to be installed.

Downloading the remote console and installing it allows you to quickly launch the remote console from the management interface and manage virtual machines.


VMware Management Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://vmwareserver.vmware.com:8222/vmware/en/
VMware Management Interface
Username:
Password:
Login
VMware Remote Console for Windows
VMware Remote Console for Windows
VMware Remote Console for Linux (tar)
VMware Remote Console for Linux (rpm)
Copyright © 1998-2003 VMware, Inc. All rights reserved.
Protected by one or more of U.S. Patent Nos. 6,397,242 and 6,496,847; patents pending.
Done
Internet

To download a package from the Login page, select it from the menu, then click **Download**.

To download a remote console package from the Status Monitor page, click the link at the bottom of the page for the appropriate installation file. This allows you to quickly download the console you need without logging out of the management interface.

Customizing the Download Menu

The download menu can be customized to suit your users' needs. For example, if your site uses the VMware Scripting APIs, you can add their installers to the download menu. Client packages containing the VMware Remote Console and the VMware Scripting APIs are available on your GSX Server CD-ROM or in the packages you downloaded from the VMware Web site. The client packages are called:

- `VMware-gsx-server-win32-client-<xxxx>.zip`
- `VMware-gsx-server-linux-client-<xxxx>.zip`

You can expand these archives and place the API installer files in a readily available area, then modify the download menu on the Login page to point to them.

You can add more files to the download menu, hide items already listed and even hide the link or the menu itself. Click the **Customize this menu** link on the Login page and follow the instructions there.

Note: On a GSX Server for Windows host with the VMware Management Interface installed, you can find the installers for the remote console and scripting APIs in `C:\Program Files\VMware\VMware Management Interface\htdocs\vmware\bin`. This folder contains:

- `VMware-console-<xxxx>.exe` — the installer for the VMware Remote Console for Windows hosts.
- `VMware-console-<xxxx>.i386.rpm` — the RPM installer for the VMware Remote Console for Linux hosts.
- `VMware-console-<xxxx>.tar.gz` — the tar installer for the VMware Remote Console for Linux hosts.
- `VMware-VmCOMAPI-<xxxx>.exe` — the installer for the VmCOM Scripting API for Windows hosts only.
- `VMware-VmPERLAPI-<xxxx>.exe` — the installer for the VmPerl Scripting API for Windows hosts.

Creating a New Virtual Machine from the Management Interface

You can create new virtual machines from within the VMware Management Interface. The process sets up a new configuration for each virtual machine you create in this fashion. You do not need to use the New Virtual Machine Wizard or Configuration Wizard in order to do this, and you can create it remotely. The virtual machines you create are located on the host to which you are currently logged in.

By default, the new virtual machine includes a SCSI disk in persistent disk mode, unless the guest operating system you select is Windows Server 2003, Windows XP, Windows Me, Windows 98 or Windows 95, in which case the virtual disk defaults to IDE. The floppy and CD-ROM drives are enabled automatically, but you can disable them.

Note: You can only use ASCII characters in the entry fields when creating a virtual machine with the management interface. Thus, the virtual machine's display name and path cannot contain non-ASCII characters.

As with any other virtual machine, you can change any configuration settings in the Configuration Editor in the local or remote console (choose **Settings** > **Configuration Editor**).

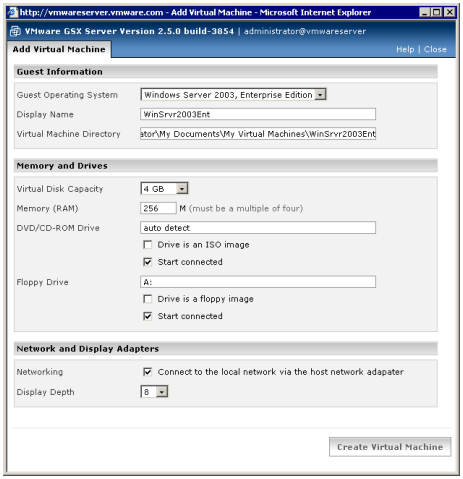
On GSX Server for Linux hosts, before you begin configuring your virtual machine, check the following items and make any necessary adjustments to the configuration of your host operating system.

- The real time clock function must be compiled into your Linux kernel.
- The parallel port "PC-style hardware" option (`CONFIG_PARPORT_PC`) must be built and loaded as a kernel module (that is, it must be set to `"m"`).

Creating a Virtual Machine

To create a virtual machine from the VMware Management Interface, complete the following steps.

1. On the Status Monitor page, click **Add Virtual Machine**. The Add Virtual Machine page appears.



2. In the **Guest Operating System** list, select the guest operating system for the new virtual machine. A display name for the operating system appears in the **Display Name** field, a default path to the configuration file appears in the **Virtual Machine Directory** field and the default amount of RAM for the operating system appears in the **Memory (RAM)** field.

   You can find detailed installation notes for each guest operating system under Installing Guest Operating Systems on page 251.

3. If you want, you can change the display name for the new virtual machine. In the **Display Name** field, type a descriptive name of the new virtual machine. This name appears in the **Display Name** column in the management interface. Remember, you can only use ASCII characters in this field.

4. If you want, you can change the path to the new virtual machine. In the **Virtual Machine Directory** field, type the path to the new virtual machine's configuration file on the host machine. Remember, you can only use ASCII characters in this field.

Each virtual machine must have its own directory. All associated files, such as the configuration file and the disk files, are placed in this directory.

5. If you want, you can change the size of the new virtual disk. In the **Virtual Disk Capacity** list, select the size of the new virtual disk. 4GB is the suggested total capacity for the virtual disk, though the maximum total capacity is 128GB for an IDE virtual disk or 256GB for a SCSI virtual disk. When you specify the size of the virtual disk, that amount of disk space is not immediately occupied by the virtual disk files. The virtual disk files grow as needed when applications and files are added to them, until the virtual disk reaches the specified maximum capacity.

   Note: If the size of the virtual disk is larger than the capacity of the host machine's hard disk, a warning message appears when you click **Create Virtual Machine**. You can ignore this message for now, since you can move this virtual machine to a different drive at a later date.

   The virtual disk's size should be large enough to hold the guest operating system and all of the software that you intend to install in the virtual machine, with room for data and growth. You cannot change the virtual disk's maximum capacity later, although you can install additional virtual disks if you run out of space on this one. For example, you need about 750MB of actual free space on the file system containing the virtual disk to install Windows 2000 inside the virtual machine.

6. If you want, you can change the amount of memory allocated to the new virtual machine. In the **Memory (RAM)** field, type the amount of RAM for the new virtual machine. VMware recommends you do not allocate less than the default listed for the guest operating system. The amount of memory you specify must be a multiple of 4.

7. Let GSX Server detect the DVD/CD-ROM drive automatically, or enter the path to the host's CD-ROM drive.

   If you want the DVD/CD-ROM drive to point to an ISO image, check **Drive is an ISO image**.

   If you want the DVD/CD-ROM drive to be connected when the virtual machine starts, check **Start connected**.

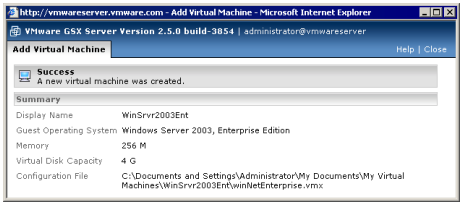
8. Enter the path to the host's floppy drive if it is different than the default.

   If you want the floppy drive to point to an ISO image, check **Drive is a floppy image**.

   If you want the floppy drive to be connected when the virtual machine starts, check **Start connected**.

9. The **Connect to the local network via the host network adapter** check box is already selected, indicating that this virtual machine is going to use bridged networking and is going to connect to your network through the host machine's Ethernet card. Uncheck the check box if you do not want to use bridged networking with this virtual machine. For more details about GSX Server networking options, see Networking on page 403.
10. If you want, you can change the color depth of your display. A higher color depth setting slows down screen redraws and increases network load when you use a remote console to view a virtual machine across a network connection. However, with greater color depth, you get better color resolution and fidelity, which may be an issue, depending on the applications you intend to run on the virtual machine. In the **Display Depth** list, select one of the following:
    - **8** - to minimize network bandwidth usage, but it is a pseudo-color or color map mode, not a true color setting.
    - **15**, **16**, or **24** - for increasingly higher true color resolution, at the expense of network bandwidth. **8** is the default setting.
11. To create your new virtual machine, click **Create Virtual Machine**.

    Note: If you do not want to create this virtual machine, click the **Close** link.
12. The Add Virtual Machine page displays a summary of the virtual machine you just created.



The new virtual machine appears on the Status Monitor page.

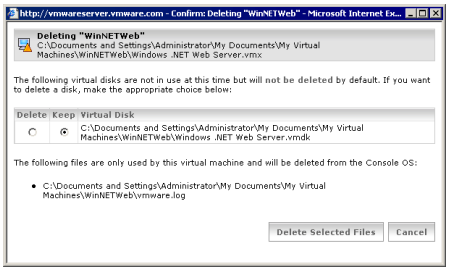
Deleting a Virtual Machine Using the VMware Management Interface

You can delete a virtual machine only if you are an administrator or root user.

When you delete a virtual machine, the files associated with it — that is, located in the same directory — are deleted. These files include its configuration file (the `.vmx` file), log file and `nvram` file. Any virtual disks that are **not** associated with another registered virtual machine on the host can be deleted as well, or you can save any or all of them for future use. The folder or directory containing these files is also deleted, unless any disk files or other files not deleted still remain.

To delete a virtual machine, complete the following steps.

1. In the VMware Management Interface, find the virtual machine you want to delete, if the virtual machine is powered on or suspended, power it off.
2. Access the virtual machine menu. Click the arrow to the right of the terminal icon ( ).
3. Choose **Delete Virtual Machine**. The Confirm: Deleting <Virtual Machine> page appears in a new window.


http://vmwareserver.vmware.com - Confirm: Deleting "WinNETWeb" - Microsoft Internet Ex...
Deleting "WinNETWeb"
C:\Documents and Settings\Administrator\My Documents\My Virtual Machines\WinNETWeb\Windows .NET Web Server.vmx
The following virtual disks are not in use at this time but will not be deleted by default. If you want to delete a disk, make the appropriate choice below:
Delete
Keep
Virtual Disk
C:\Documents and Settings\Administrator\My Documents\My Virtual Machines\WinNETWeb\Windows .NET Web Server.vmdk
The following files are only used by this virtual machine and will be deleted from the Console OS:
C:\Documents and Settings\Administrator\My Documents\My Virtual Machines\WinNETWeb\vmware.log
Delete Selected Files
Cancel

4. All the files that are to be deleted are listed. For each disk file not associated with another registered virtual machine on this host, choose one of the following:
   - To save a virtual disk file, select the **Save** option.
   - To delete a virtual disk file, select the **Delete** option.

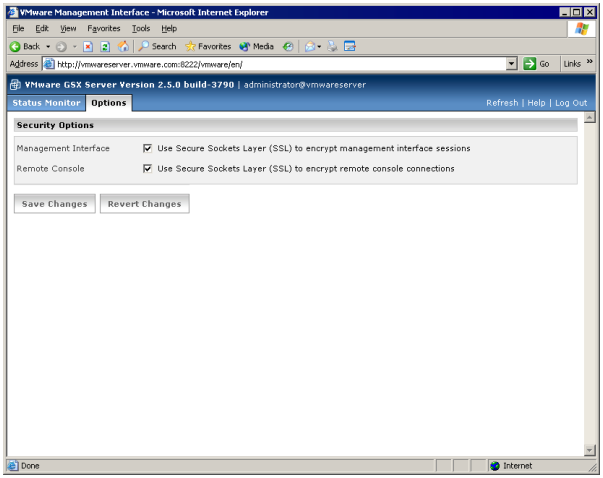
   Note: Any virtual disk files associated with another registered virtual machine do not appear in this window.
5. When you are ready to delete the virtual machine, click **Delete Selected Files**. The Confirm: Deleting <Virtual Machine> page closes. The virtual machine no longer appears in the management interface.

   Note: If you do not want to delete this virtual machine, click **Cancel**.

Configuring the VMware GSX Server Host

To configure certain GSX Server settings, on the Status Monitor page, click the **Options** tab. The Options page appears.

Note: Only a user with administrator privileges (Windows hosts) or the root user (Linux hosts) can access this tab.


VMware Management Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://vmwareserver.vmware.com:8222/vmware/en/
Go Links
VMware GSX Server Version 2.5.0 build-3790 | administrator@vmwareserver
Status Monitor Options
Refresh | Help | Log Out
Security Options
Management Interface
Use Secure Sockets Layer (SSL) to encrypt management interface sessions
Remote Console
Use Secure Sockets Layer (SSL) to encrypt remote console connections
Save Changes
Revert Changes
Done
Internet

On this page are options that allow you to use secure sockets layer (SSL) to secure your VMware Management Interface sessions and VMware Remote Console connections. For more information, see Securing Your Remote Sessions on page 153.

Click the **Status Monitor** tab to return to the Status Monitor page.

Logging Out of the VMware Management Interface

When you are ready to log out of the VMware Management Interface, click **Logout** on the Status Monitor or Options page. You are prompted to confirm that you want to log out. Logging out does not affect the virtual machines on the host or any remote consoles you opened from the management interface.

VMware Management Interface sessions expire automatically after 60 minutes of inactivity or idle time.

The Apache Server and the Management Interface

On GSX Server for Linux hosts, an Apache server is installed with the VMware Management Interface. Listed here are the commands to start, stop or restart the Apache server. In order to use these commands, you must first log in as root (`su -`).

To start the Apache server, type
`/etc/init.d/httpd.vmware start`

To stop the Apache server, type
`/etc/init.d/httpd.vmware stop`

To restart the Apache server, type
`/etc/init.d/httpd.vmware restart`

Setting a MIME Type to Launch the VMware Remote Console

From a browser, you can connect to a virtual machine from a remote console by clicking the terminal icon ( ) for that virtual machine. Before doing so, Netscape and Mozilla users need to define a MIME type of `x-vmware-console` and associate it with the remote console program file. Internet Explorer is automatically configured when you install the console.

Setting the MIME Type in Netscape 7.0 and Mozilla 1.x

If you are using Netscape 7.0 or Mozilla 1.x and want to launch the VMware Remote Console from the VMware Management Interface, you must first set a MIME type for the remote console program.

The procedure is similar for Windows and Linux hosts. Both involve writing a short script that provides the command to launch the remote console.

In Netscape or Mozilla, follow these steps to set the MIME type.

1. Open a text editor and do one of the following.
   - On a Windows host, write a short batch file called `vmwareConsole-helper.bat`. The batch file must contain the following line:
     `"<path_to_vmwareConsole>" -o "%1"`
     Where the default `<path_to_vmwareConsole>` is
     `C:\Program Files\VMware\VMware Remote Console\vmwareConsole.exe`

- On a Linux host, write a short shell script called `vmware-console-helper.sh`. The shell script must contain the following two lines:
  ```
  #!/bin/sh
  "<path_to_vmware-console>" -o $1 > /dev/null 2>&1;
  ```
  Where the default `<path_to_vmware-console>` is `/usr/bin/vmware-console`.

2. Save the file in a location of your choice.

   Note: On a Linux host, change to the directory where you saved the file and give yourself permission to execute the file.

   ```
   chmod +x vmware-console-helper.sh
   ```

3. Use the browser to connect to the server you want to manage.
4. Click the terminal icon ( ) for the virtual machine you want to view in a remote console.
5. A dialog box asks what you want to do with the file. Click **Advanced**.
6. In the New Type dialog box, in the **Description of type** field, type `VMware Remote Console`.
7. In the **File extension** field, type `xvm`.
8. In the **MIME type** field, type `application/x-vmware-console`.
9. In the **Application to use** field, type the path to `vmwareConsole-helper.bat` or `vmware-console-helper.sh`.
10. Click **OK** twice. Your browser is now set to launch the remote console when you click the terminal icon in the future.

7

Using Local and Remote Consoles

Using Local and Remote Consoles

This section describes how to use local and remote consoles:

- Connecting to Virtual Machines from Local and Remote Consoles on page 187
  - How to Run a VMware GSX Server Console on page 187
  - Starting the Local Console on a Windows Host on page 188
  - Starting the Local Console on a Linux Host on page 188
  - Starting the Remote Console on a Windows Remote Workstation on page 189
  - Starting the Remote Console on a Linux Remote Workstation on page 190
  - Using the Local or Remote Console on page 191
  - Powering On Virtual Machines from a Local Console on page 194
  - Special Power Options for Virtual Machines on page 195
  - Instantly Restoring a Virtual Machine on page 197
  - Displaying the Remote Console Banner on page 198
  - Changing the Port Number for Remote Console Connections on page 198
  - Upgrading the VMware Remote Console on page 201
- Specifying GSX Server Preferences from a Console on page 207
  - Setting Input Preferences on page 207
  - Setting Hot-Key Preferences on page 210
  - Setting Priority Preferences on page 212
  - Setting Memory Preferences on page 214
  - Setting Workspace Preferences on page 216
- Closing a Console on page 217

Connecting to Virtual Machines from Local and Remote Consoles

How to Run a VMware GSX Server Console

There are three ways to run a console in GSX Server:

- With the VMware Remote Console on a Windows or Linux workstation. This allows you to manage a virtual machine remotely. Remote consoles permit shared access to and control of the same virtual machine; other remote consoles can connect to a virtual machine to which you already are connected. When all remote consoles are disconnected from a virtual machine, the virtual machine continues to run, headless.

  Windows and Linux versions of the VMware Remote Console are available. You can run the remote console on Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0 or Linux computers. The VMware Remote Console is installed automatically on the GSX Server for Windows host if you chose a complete installation.
- With the VMware Remote Console on the GSX Server host. This can be done when other remote consoles are connected to the virtual machine to which you want to connect.
- With the local console on the GSX Server host. This can be done only when no VMware Remote Consoles or VMware Scripting APIs are connected to the virtual machine to which you want to connect. Before starting the local console, you must gracefully shut down the virtual machine and close all remote console windows, unless it is already powered off.

  You use a local console when you need exclusive access to a virtual machine. You need exclusive access when you want to install the guest operating system inside the virtual machine, if you need better performance than the VMware Remote Console or to run the virtual machine in full screen mode for even better performance. The local console is installed automatically on the server where you installed GSX Server, and you run it locally on the server host.

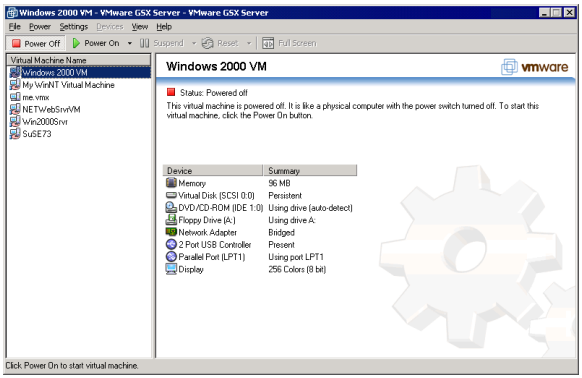
Starting the Local Console on a Windows Host

1. If the virtual machine is already running, gracefully suspend it or shut it down and disconnect all consoles and VMware Scripting APIs.
2. Launch the local console at the server host.

   Start > **Programs** > **VMware** > **VMware GSX Server**

   (Or, double-click the VMware GSX Server icon on your desktop.)

   The local console window opens.

3. In the Virtual Machine Name list, select a virtual machine. You can power it on, resume it (if it was suspended in a local console) or change its configuration.
   - To power on or resume the virtual machine, see Using the Local or Remote Console on page 191.
   - To change its configuration, right-click the virtual machine name in the **Virtual Machine Name** list and choose **Settings**. The Configuration Editor opens.

Starting the Local Console on a Linux Host

1. If the virtual machine is already running, gracefully suspend it or shut it down and disconnect all consoles and VMware Scripting APIs.
2. Launch the local console at the GSX Server host machine.

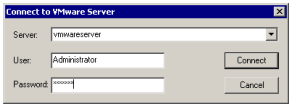
   ```
   vmware -G /<path_to_config_file>/<config_file>.cfg
   ```

Starting the Remote Console on a Windows Remote Workstation

1. To start the VMware Remote Console, do one of the following:
   - Choose **Start** > **Programs** > **VMware** > **VMware Remote Console**.
   - On your desktop, double-click the VMware Remote Console icon.

   - In the VMware Management Interface, click the terminal icon ( ) to launch a remote console for that virtual machine. If you are connected to the management interface in a Netscape or Mozilla browser, you must define a MIME type and associate it with the remote console program. For instructions, see Setting a MIME Type to Launch the VMware Remote Console on page 183.

   The Connect to VMware Server dialog box appears.

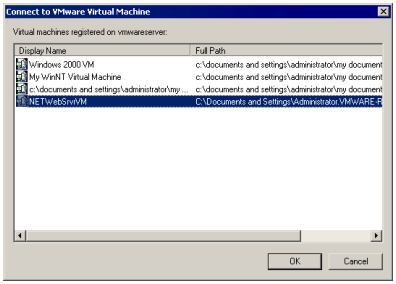
   

2. The dialog box asks for the information necessary for you to connect to the virtual machine. Enter
   - The server host name (or IP address)
   - Your user name on that server
   - Your password

   Hint: To save yourself a step, in the **Server** field, specify the path to the configuration file for the virtual machine to which you are connecting. You connect to the virtual machine automatically when you click Connect, and can skip the remaining steps.

   Note: GSX Server connects to this server through port 902 by default; if you want to connect to a different port, add this number after the server name. For example, to connect to the virtual machine through port 932, you can type:
   `hostserver.domain 932 <path_to_the_config_file>`
   (remember, the configuration file path is optional)
   This port can be changed in case your site uses port 902 for another application; for more information, see Changing the Port Number for Remote Console Connections on page 198.

3. Click **Connect**. The Connect to VMware Virtual Machine dialog box appears.



4. In the dialog box is a list of all virtual machines that are registered on the server host, identified by their display names and paths to their configuration files. In the list, select the virtual machine to which you want to connect and click **OK**. The remote console window opens with the virtual machine in its current state (powered on, suspended or powered off).

Starting the Remote Console on a Linux Remote Workstation

1. To start the VMware Remote Console, do one of the following:
   - At a command prompt, type `vmware-console`.

     Note: If you put the path to the configuration file in the command line, the virtual machine opens in the remote console. Otherwise, proceed to step 2.
   - In the VMware Management Interface, click the terminal icon ( ) to launch a remote console for that virtual machine. If you are connected to the management interface in a Netscape or Mozilla browser, you must define a MIME type and associate it with the remote console program. For instructions, see Setting a MIME Type to Launch the VMware Remote Console on page 183.
2. A dialog box asks for the information to connect you to the virtual machine. Enter
   - The server host name (or IP address)
   - Your user name on that server
   - Your password

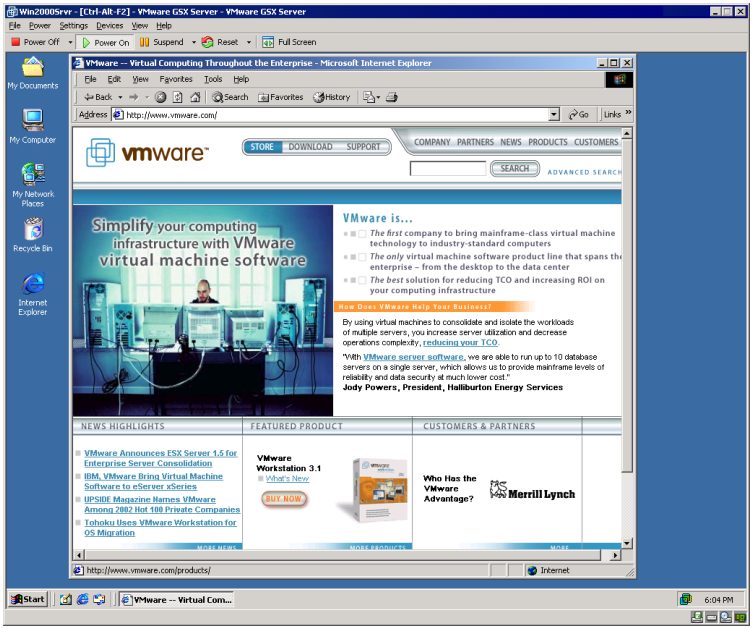
   Note: GSX Server connects to this server through port 902 by default; if you want to connect to a different port, add this number after the server name. For example, to connect to the virtual machine through port 932, you can type:
   `hostserver.domain 932 <path_to_the_config_file>`

(remember, the configuration file path is optional)
This port can be changed in case your site uses port 902 for another application; for more information, see Changing the Port Number for Remote Console Connections on page 198.

3. Click **OK**. The Connect to VMware Virtual Machine dialog box appears.
4. In the dialog box is a list of all virtual machines that are registered on the server host, identified by their display names and paths to their configuration files. In the list, select the virtual machine to which you want to connect and click **OK**. The remote console window opens with the virtual machine in its current state (powered on, suspended or powered off).

Using the Local or Remote Console

When you view a virtual machine through a local or remote console, it behaves much like a physical computer that runs in a window on your computer's desktop.


Win2000Srvr - [Ctrl-Alt-F2] - VMware GSX Server - VMware GSX Server
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
VMware -- Virtual Computing Throughout the Enterprise - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.vmware.com/
vmware
STORE DOWNLOAD SUPPORT
COMPANY PARTNERS NEWS PRODUCTS CUSTOMERS
SEARCH
ADVANCED SEARCH
Simplify your computing infrastructure with VMware virtual machine software
VMware is...
The first company to bring mainframe-class virtual machine technology to industry-standard computers
The only virtual machine software product line that spans the enterprise – from the desktop to the data center
The best solution for reducing TCO and increasing ROI on your computing infrastructure
How Does VMware Help Your Business?
By using virtual machines to consolidate and isolate the workloads of multiple servers, you increase server utilization and decrease operations complexity, reducing your TCO.
"With VMware server software, we are able to run up to 10 database servers on a single server, which allows us to provide mainframe levels of reliability and data security at much lower cost."
Jody Powers, President, Halliburton Energy Services
NEWS HIGHLIGHTS
FEATURED PRODUCT
CUSTOMERS & PARTNERS
VMware Announces ESX Server 1.5 for Enterprise Server Consolidation
IBM, VMware Bring Virtual Machine Software to eServer zSeries
UPSIDE Magazine Names VMware Among 2002 Hot 100 Private Companies
Tohoku Uses VMware Workstation for OS Migration
VMware Workstation 3.1
What's New
BUY NOW
Who Has the VMware Advantage?
Merrill Lynch
http://www.vmware.com/products/
Internet
Start
VMware -- Virtual Com...
6:04 PM
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer

Depending on your permissions, you may not be able to perform certain activities in a console, such as saving a configuration as a new configuration file or accessing the Configuration Editor. For more information about permissions, see Securing Your Virtual Machines on page 148.

Instead of using physical buttons to turn this computer on and off, you use buttons in the toolbar at the top of the console window.

Windows 2000 VM - [Ctrl-Alt-F1] - VMware GSX Server - VMware GSX
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset

Local console toolbar when virtual machine is powered off (Windows host)

Toolbar when virtual machine is powered off (Linux host)

Windows 2000 VM - [Ctrl-Alt-F1] - VMware GSX Server - VMware GSX
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset

Local console toolbar when virtual machine is powered on (Windows host)

Toolbar when virtual machine is powered on (Linux host)

Local console toolbar when virtual machine is suspended (Windows host)

Toolbar when virtual machine is suspended (Linux host)

On a Windows host, there are separate **Power Off** and **Power On** buttons. When you suspend a virtual machine, the **Power On** button becomes a **Resume** button. In addition, each button has an arrow next to it that, when clicked, opens a menu of sub-options related to the power button. These options are also available on the **Power** menu. For more information, see Special Power Options for Virtual Machines on page 195.

On a Linux host, the power button is labeled **Power On** or **Power Off**, depending on whether your virtual machine is running or not. There are special power options available on the **Power** menu. For more information, see Special Power Options for Virtual Machines on page 195.

On a Windows host, an alert appears at the bottom left corner of the GSX Server console window when your virtual machine is not running the version of VMware Tools that matches your version of GSX Server.

You see a small icon and a note you can click to begin installing VMware Tools. This gives you a quick way to launch the VMware Tools installer. It is especially useful immediately after you install the guest operating system in a new virtual machine.

On a Linux host, a note in the bottom bar of the GSX Server console window alerts you when your virtual machine is not running the version of VMware Tools that matches your version of GSX Server. To launch the VMware Tools installer, choose **Settings** > **VMware Tools Install**.

Note: Your guest operating system must be completely installed and running when you install VMware Tools.

For details, see Installing VMware Tools on page 113.

Once you power on the virtual machine, you can interact with it just as you do with a physical computer. In addition, you can take advantage of the special capabilities specific to virtual machines. For more information on these capabilities, see Running Virtual Machines on page 219.

Powering On Virtual Machines from a Local Console

When you connect to a virtual machine with a local console, you have exclusive access to the virtual machine. As long as you stay connected with the local console, no one else can connect to it, either with another local console, a remote console or VMware Scripting API, nor can you change its power state (power it on or off, suspend or resume it) with the VMware Management Interface. Remote management is not possible when you are connected through the local console.

For a local console on a Windows host, you can choose to power on a virtual machine for local or remote management. When you power on the virtual machine for remote management it starts headless; that is, without the local console. The virtual machine does not open in the local console, but any user can now connect to the virtual machine with a remote console.

- To power on a virtual machine so you have exclusive access to the virtual machine, on the local console's toolbar, click the arrow next to the **Power On** button and select **Power On For Local Management**. The virtual machine powers on in the local console window. On a Windows local console, this is the same as clicking the toolbar's **Power On** button.
- To power on a virtual machine headless, so everyone has access to the virtual machine, on the local console toolbar, click the arrow next to the **Power On** button and select **Power On For Remote Management**. The virtual machine powers on, running headless, ready to be connected to with remote consoles. The local console remains open.

On a Linux host, you can power on a virtual machine headless. From a command prompt, type:

```
vmware -x <configfile>.cfg
```

Special Power Options for Virtual Machines

When VMware Tools is running, you can run scripts when you change the power state of a virtual machine; that is, when you power on, power off, suspend or resume the virtual machine. For more information, see Executing Scripts When the Virtual Machine's Power State Changes on page 122.

When you reset a virtual machine, you can choose to restart the guest operating system, which gracefully closes applications and restarts the guest operating system, or reset the virtual machine, which is the same as pressing the reset button on a physical computer.

Similarly, when you power off the virtual machine, you can choose to shut down the guest operating system, which gracefully closes applications and shuts the guest operating system down, or turn off the virtual machine, which is the same as pressing the power button on a physical computer.

All the power options are available on the Power menu. Each menu item corresponds to a button on the toolbar, and opens a submenu containing the associated options. The menu items may not be available, depending upon the current power state of the virtual machine. For example, if the virtual machine is powered off, you cannot select any power off, suspend, resume or reset options.

On a Windows host, these power options are also available on the toolbar. Each power button has an arrow next to it. Click the arrow to open a menu of options related to that power button.

Options for Powering On a Virtual Machine

From a local console, you can choose from the following options when powering on a virtual machine:

- Power On For Local Management — powers on the virtual machine in the local console. This is the same as clicking the **Power On** button on the toolbar.
- Power On For Local Management Then Run Script — powers on the virtual machine in the local console, then executes the associated script.
- Power On For Remote Management — powers on the virtual machine headless. The virtual machine powers on, but does not open in a console window. The virtual machine can be connected to with remote consoles. The local console remains open.

From a remote console, you can choose from the following options when powering on a virtual machine:

- Power On Virtual Machine — powers on the virtual machine in the remote console. This is the same as clicking the **Power On** button on the toolbar.
- Power On Then Run Script — powers on the virtual machine in a remote console, then executes the associated script.

Options for Powering Off a Virtual Machine

You can choose from the following options when powering off a virtual machine:

- Power Off Virtual Machine — powers off the virtual machine. This is similar to turning off a physical computer by pressing its power button, so any programs running in the virtual machine may be adversely affected. Clicking the **Power Off** button on the toolbar powers off the virtual machine.
- Shut Down Guest Operating System — gracefully shuts the guest operating system down and, if the guest operating system supports Advanced Power Management, powers off the virtual machine. If there is a script associated with this power operation, it executes after the shut down begins. This is the same as choosing **Start** > **Shut Down** > **Shut Down** in a Windows operating system or issuing a `shutdown` command in a Linux operating system.

Options for Suspending a Virtual Machine

You can choose from the following options when suspending a virtual machine:

- Run Script Then Suspend — executes the associated script, then suspends the virtual machine. This is the same as clicking **Suspend** on the toolbar, unless a script is not associated with suspending a virtual machine.
- Suspend Virtual Machine — suspends the virtual machine.

Options for Resuming a Virtual Machine

You can choose from the following options when resuming a virtual machine:

- Resume Then Run Script — resumes the suspended virtual machine, then executes the associated script. This is the same as clicking **Resume** on the toolbar, unless a script is not associated with resuming a virtual machine.
- Resume Virtual Machine — resumes the suspended virtual machine.

Options for Resetting a Virtual Machine

You can choose from the following options when resetting a virtual machine:

- **Reset Virtual Machine** — resets the virtual machine. This is similar to resetting a physical computer by pressing its reset button, so any programs running in the virtual machine may be adversely affected. Clicking the **Reset** button on the toolbar resets the virtual machine.
- **Restart Guest Operating System** — gracefully restarts the virtual machine. This is the same as choosing **Start** > **Shut Down** > **Restart** in a Windows operating system or issuing a `reboot` command in a Linux operating system.

Special power operations can be performed from the VMware Management Interface. For more information, see Using the Status Monitor on page 165.

Instantly Restoring a Virtual Machine

Another quick way to resume a virtual machine in the local console is to use the instant restore feature.

The instant restore feature can resume a virtual machine that is suspended. Choose **File** > **Instant Restore** and select the virtual machine to resume. If the virtual machine is not suspended, the operation fails.

Note: If you are running a virtual machine in a local console and instantly restore another virtual machine, the virtual machine currently running is suspended and the one you are instantly restoring resumes in the same local console.

Displaying the Remote Console Banner

In order to better distinguish between the local and remote consoles, you can display a banner across the top of the display area of the remote console window installed on a Windows host. This enlarges the remote console window slightly; it does not cover up your virtual machine's display.

To display the remote console banner, choose **View** > **Remote Console Banner**.

Windows 2000 Professional - vmwareserver.vmware.com VMware GSX Server - VMware ...
File Power Settings Devices View Help
Power Off Resume Suspend Reset Detach and Exit
VMware GSX Server: vmwareserver.vmware.com
remote console
Windows 2000 Professional
vmware
Status: Suspended
This virtual machine is suspended. You can start it quickly and begin working with all applications and documents in the same state they were in when you suspended the virtual machine. To start this virtual machine, click the Resume button.
If you were using USB devices at the time you suspended the virtual machine, you can reconnect them using the Devices menu.
Device
Summary
Memory
192 MB
Virtual Disk (SCSI 0:0)
Persistent
DVD/CD-ROM (IDE 1:0)
Using drive (auto-detect)
Floppy Drive (A:)
Using drive A:
Network Adapter
Bridged
2 Port USB Controller
Present
Display
High Color (16 bit)
Click Resume to resume virtual machine.

Remote console window with its banner displayed.

To hide the remote console banner, choose **View** > **Remote Console Banner** again.

Changing the Port Number for Remote Console Connections

By default, the VMware Remote Console connects to virtual machines over port 902. If this port assignment poses a conflict for your site, for example, if you use the *ideafarm-chat* program, you can change the port number the remote console uses accordingly.

Changing the port number involves manually adding a variable to certain preference files. The steps you need to take vary depending upon the server host operating system, the host on which the console is running and whether you are making this change to GSX Server itself (by assigning the new port number to a variable called `authd.port`) or to the remote console (by assigning the new port number to a variable called `authd.client.port`).

The setting for `authd.port` is different from the setting for `authd.client.port`. The `authd.port` variable tells GSX Server (the server side) what port to listen to for remote console connections. The `authd.client.port` variable tells the remote console (the client side) the port with which to connect. Thus, if you set only `authd.port` to a different port number,

such as 9902, and you try to connect to a virtual machine on that host with a remote console, the console still tries to connect to port 902. Keep in mind that you can still substitute this new port number manually when you connect with a remote console. In the Connect to VMware Server dialog box, in the **Server** field, enter the port number along with the name of the GSX Server host name and configuration file path, like this:

```
<server name> <port> <config file>
```

Depending upon your site's needs or configuration (for instance, you have multiple GSX Server hosts and they use different ports), this might be acceptable. However, for seamless integration between the server and the remote console, and to avoid manual entry of the port number every time a remote console connects, if you want to use a port other than 902, then you should set `authd.client.port` to the same port number you use for `authd.port`.

Changing the Port Number on a Windows Host

- To change the port number on the GSX Server for Windows host, you must create a file called `config.ini` and place it in `C:\Documents and Settings\All Users\Application Data\VMware\VMware GSX Server` (Windows Server 2003 and Windows 2000 hosts); on a Windows NT host, the file must be placed in `C:\WINNT\Profiles\<user>\Application Data\VMware`. In this file set the new port number to the `authd.port` variable. All remote consoles connecting to virtual machines on this host must use this port number.
- To change the port number which is used by the remote console installed on a Windows host, you must create a file called `config.ini` and place it in `C:\Documents and Settings\All Users\Application Data\VMware\VMware Remote Console` (Windows Server 2003 and Windows 2000 hosts); on a Windows NT host, the file must be placed in `C:\WINNT\Profiles\<user>\Application Data\VMware`. In this file set the new port number to the `authd.client.port` variable. All remote consoles on this machine connecting to virtual machines on the VMware GSX Server host use this port number. The VMware GSX Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).
- To change the port number for a specific user who is using the remote console installed on a Windows host, you need to set the new port number to the `authd.client.port` variable in the `preferences.ini` file located in `C:\Documents and Settings\<user>\Application`

Data\VMware (Windows Server 2003, Windows XP and Windows 2000 hosts); on a Windows NT host, the file is located in C:\WINNT\Profiles\<user>\Application Data\VMware. Only when this user is logged in and using a remote console to connect to a virtual machine on the GSX Server host is this port number used. The GSX Server host must have this port number set to the authd.port variable in its config.ini file (Windows host) or vmware-authd file (Linux host).

Changing the Port Number on a Linux Host

- To change the port number on the GSX Server for Linux host, you first need to determine whether your host is configured to use xinetd or inetd. If your host is configured to use xinetd, change the port number in the port = 902 line in the vmware-authd file located in /etc/xinetd. Otherwise, if you host is configured to use inetd, change the port number in the 902 ... vmware-authd line in /etc/inetd.conf. All remote consoles connecting to virtual machines on this host must use this port number.
- To change the port number which is used by the remote console installed on a Linux host, you must set the new port number to the authd.client.port variable in either of the following files:

  /etc/vmware-console/config

  /usr/lib/vmware-console/config

  All remote consoles on this machine connecting to virtual machines on the GSX Server host use this port number. The GSX Server host must have this port number set to the authd.port variable in its config.ini file (Windows host) or vmware-authd file (Linux host).

  Note: If the port number specified in these files is different, the port number specified in /etc/vmware-console/config takes precedence.
- To change the port number for a specific user who is using the remote console installed on a Linux host, you need to set the new port number to the authd.client.port variable in ~/.vmware/preferences. Only when this user is logged in and using a remote console to connect to a virtual machine on the GSX Server host is this port number used. The GSX Server host must have this port number set to the authd.port variable in its config.ini file (Windows host) or vmware-authd file (Linux host). When this user is logged in, the port number specified in ~/.vmware/preferences supersedes the port number specified in /etc/vmware-console/config or /usr/lib/vmware-console/config.

Substituting a Port Number with the VMware Scripting APIs

With the VMware Scripting APIs, you can supply a different port number when you create a new virtual machine object. This port number must match the port number on the GSX Server host set to the `authd.port` variable in the `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

If you specify 0 as the port number, the port number specified by `authd.client.port` is used instead. If `authd.client.port` is not specified, the default port 902 is used.

For more information, visit the VMware Web site at *www.vmware.com/support/developer*.

Upgrading the VMware Remote Console

You cannot connect to a virtual machine on a GSX Server or VMware ESX Server host with a remote console that is from a build older than the server build. You must upgrade the remote console to match the version of GSX Server or ESX Server to which you are connecting.

First, uninstall the current remote console. Then connect to the GSX Server or ESX Server host with the VMware Management Interface and download the console installation package from the Login page. GSX Server for Windows users can use the custom path with the GSX Server Master Installer.

Uninstalling a Windows Remote Console

The easiest way to uninstall the remote console on a Windows host is to use Add/Remove Programs in the Windows Control Panel.

1. Choose **Start** > **Settings** > **Control Panel**.
2. Double click **Add/Remove Programs** (**Add or Remove Programs** on a Windows Server 2003 host).
3. Select VMware Remote Console.
4. For Windows Server 2003 or Windows XP, click **Remove**. For Windows 2000, click **Change/Remove**. For Windows NT 4.0, click **Add/Remove**.
5. Follow the on-screen instructions.

Uninstalling a Linux Remote Console

To uninstall a Linux remote console that was installed from a tar package, run `/usr/bin/vmware-uninstall-console.pl`

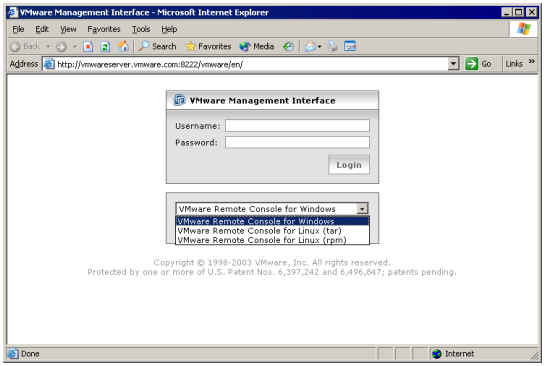
To uninstall a Linux remote console that was installed from an RPM package, type `rpm -e VMware-console`

Downloading and Installing the VMware Remote Console from the VMware Management Interface

If you download the remote console installer from the management interface, complete the following steps to install the remote console.

- You can download the installer from the VMware Management Interface. In the menu on the Login page, or at the bottom of the Status Monitor page, click the appropriate link for the host operating system of the machine on which you want to run the console.

1. Connect to the VMware GSX Server host with the VMware Management Interface. For information on connecting to the management interface, see Logging In to the VMware Management Interface on page 163.


VMware Management Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://vmwareserver.vmware.com:8222/vmware/en/
VMware Management Interface
Username:
Password:
Login
VMware Remote Console for Windows
VMware Remote Console for Windows
VMware Remote Console for Linux (tar)
VMware Remote Console for Linux (rpm)
Copyright © 1998-2003 VMware, Inc. All rights reserved.
Protected by one or more of U.S. Patent Nos. 6,397,242 and 6,496,847; patents pending.
Done
Internet

2. On the Login page, select the remote console installation package appropriate to the operating system on which it is to be installed. If you are installing the console on a Linux host, you can further choose between tar and RPM installation packages.

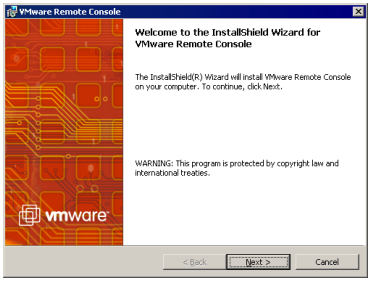
   Note: You can also download the remote console installation packages from the Status Monitor page in the management interface.

3. Click **Download**.
4. Run the installation package.

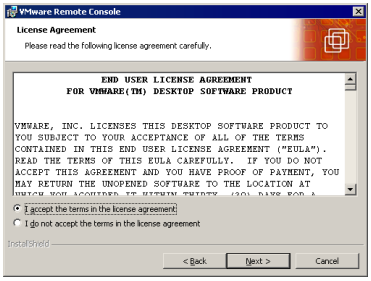
   To install the remote console on a Linux host, see Installing the VMware Remote Console on a Linux Host on page 63.

   To start the installation wizard on a Windows host, from the directory where you downloaded the installer, run `VMware-console-<xxxx>.exe`, where

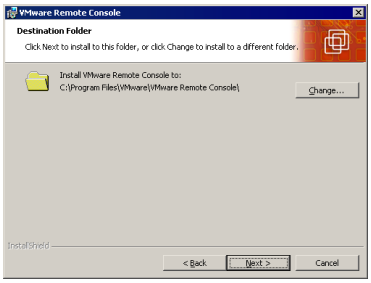
<xxxx> is a series of numbers representing the version and build numbers. The InstallShield Wizard dialog appears. Click **Next**.


VMware Remote Console
Welcome to the InstallShield Wizard for VMware Remote Console
The InstallShield(R) Wizard will install VMware Remote Console on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
vmware
< Back
Next >
Cancel

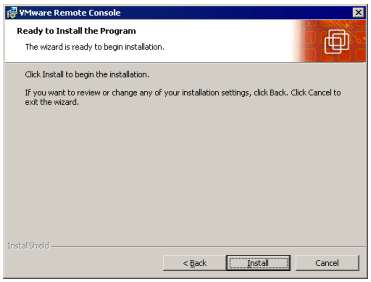
5. Accept the End User License Agreement. Select **I accept the terms in the license agreement**, then click **Next**.


VMware Remote Console
License Agreement
Please read the following license agreement carefully.
END USER LICENSE AGREEMENT
FOR VMWARE(TM) DESKTOP SOFTWARE PRODUCT
VMWARE, INC. LICENSES THIS DESKTOP SOFTWARE PRODUCT TO YOU SUBJECT TO YOUR ACCEPTANCE OF ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT ("EULA"). READ THE TERMS OF THIS EULA CAREFULLY. IF YOU DO NOT ACCEPT THIS AGREEMENT AND YOU HAVE PROOF OF PAYMENT, YOU MAY RETURN THE UNOPENED SOFTWARE TO THE LOCATION AT
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

6. Choose the directory in which to install the remote console. If you prefer to install it in a directory other than the default, click **Change** and change to your directory of choice. If the directory does not exist, it is created for you. Click **Next**.

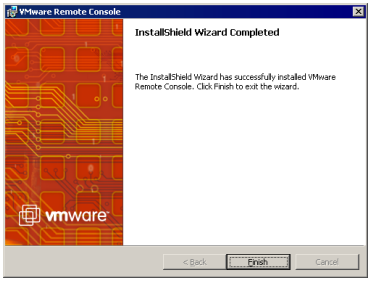

VMware Remote Console
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install VMware Remote Console to:
C:\Program Files\VMware\VMware Remote Console\
Change...
InstallShield
< Back
Next >
Cancel

7. If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the dialog box containing the information you want to change.


VMware Remote Console
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

   Otherwise, click **Install**. The installer begins copying files to your host.

8. When the setup completes, click **Finish**. You do not need to reboot your host operating system after you install the remote console.



Installing the Remote Console from the GSX Server Master Installer

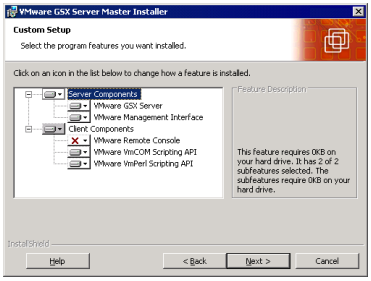
GSX Server for Windows users can use the GSX Server Master Installer to install the remote console. The master installer must be located on the system on which you want to install the remote console.

1. Choose **Start** > **Settings** > **Control Panel**.
2. Double click **Add/Remove Programs** (**Add or Remove Programs** on a Windows Server 2003 host).
3. Select **VMware GSX Server Master Installer** and click **Change**.
4. The GSX Server Master Installer starts. Click **Next**.

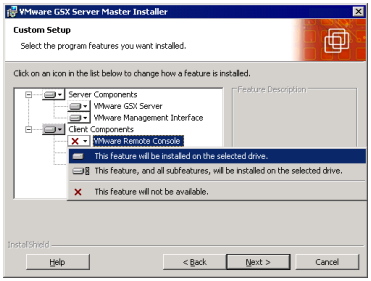
5. Click **Modify**, then click **Next**.

VMware GSX Server Master Installer
Program Maintenance
Modify, repair, or remove the program.
Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
Repair
Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.
Remove
Remove all GSX Server components from your computer.
InstallShield
< Back
Next >
Cancel

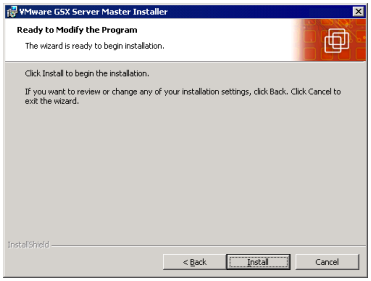
6. The master installer shows all the components that are currently installed on the system. Any components not installed are indicated by a red X to the left of the component. In this case, the remote console is not installed.


VMware GSX Server Master Installer
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Server Components
VMware GSX Server
VMware Management Interface
Client Components
VMware Remote Console
VMware VmCOM Scripting API
VMware VmPerl Scripting API
Feature Description
This feature requires 0KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 0KB on your hard drive.
InstallShield
Help
< Back
Next >
Cancel

7. Click the arrow next to **VMware Remote Console**. A popup menu appears. Choose **This feature will be installed on the selected drive**. Click **Next**.


VMware GSX Server Master Installer
Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Server Components
VMware GSX Server
VMware Management Interface
Client Components
VMware Remote Console
This feature will be installed on the selected drive.
This feature, and all subfeatures, will be installed on the selected drive.
This feature will not be available.
Feature Description
InstallShield
Help
< Back
Next >
Cancel

8. The installer is ready to install the remote console. Click **Install**. The remote console is installed and the master installer closes.


VMware GSX Server Master Installer
Ready to Modify the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

Specifying GSX Server Preferences from a Console

In a local console, for each user, you can specify GSX Server configuration settings that are global, that is, they affect all virtual machines on a host. You can also specify settings particular to the virtual machine to which the console is connected.

To set preferences, in a console window, choose **Settings** > **Preferences** in a Windows console or **Settings** > **Input Preferences** in a Linux console. The Preferences dialog box appears.

From the local console, you can specify the following preferences:

- Setting Input Preferences on page 207
- Setting Hot-Key Preferences on page 210
- Setting Priority Preferences on page 212 (Windows hosts only)
- Setting Memory Preferences on page 214
- Setting Workspace Preferences on page 216 (Windows hosts only)

From a remote console, you can specify only input and hot-key preferences.

Setting Input Preferences

To direct input to the virtual machine, GSX Server grabs the keyboard and the mouse so all keystrokes, mouse moves and button clicks go to the virtual machine.

You can choose when GSX Server starts grabbing input:

- When you click the mouse in the console window
- When you type in the console window
- When you click or type in the console window

When an on-mouse click option is selected, GSX Server grabs the keyboard and the mouse on the first left mouse button click in the virtual machine's console window. The first click in the window is not sent to the virtual machine.

When an on-key press option is selected, GSX Server grabs the keyboard and the mouse on the first keystroke. The first keystroke is sent to the virtual machine. When the console window is active and on key press selected, there is no way to use the normal application and system accelerator key sequences.

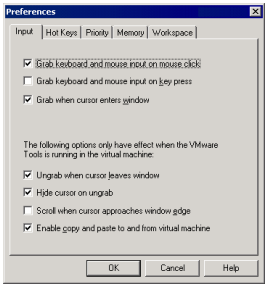
Cursor Options

The best way to understand the cursor options is to play with them for a while. They describe how the mouse pointer should behave when you are in windowed mode; that is, the virtual machine is in a console window, not in full screen mode, and you can see the rest of your host operating system's desktop.

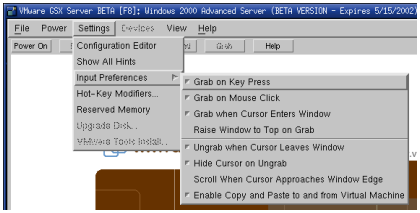
Changing Your Input Settings

The **Settings** menu allows you to change a number of settings that apply to GSX Server itself, no matter what virtual machine you are running.

To make changes to these settings on a Windows host, choose **Settings** > **Preferences**. The **Input** tab on a Windows host lets you adjust the way that the virtual machine captures control of the mouse and keyboard.


Preferences
Input
Hot Keys
Priority
Memory
Workspace
Grab keyboard and mouse input on mouse click
Grab keyboard and mouse input on key press
Grab when cursor enters window
The following options only have effect when the VMware Tools is running in the virtual machine:
Ungrab when cursor leaves window
Hide cursor on ungrab
Scroll when cursor approaches window edge
Enable copy and paste to and from virtual machine
OK
Cancel
Help

To change the input settings on a Linux host, choose **Settings** > **Input Preferences**, then click an item on the cascading menu to toggle its setting on or off.



The input settings you can specify include:

- **Grab keyboard and mouse input on mouse click** — GSX Server grabs the keyboard and the mouse after the first primary mouse button click in the virtual machine console window.
- **Grab keyboard and mouse input on key press** — GSX Server grabs the keyboard and the mouse after the first keystroke. The first keystroke is sent to the

virtual machine. When the virtual machine console window is active and this option is selected, there is no way to use the normal application and system accelerator key sequences.

- **Grab when cursor enters window** — the mouse pointer becomes the mouse pointer of your guest operating system when the mouse pointer enters the virtual machine console window. This does not apply in full screen mode.
- **Ungrab when cursor leaves window** — the mouse pointer becomes the mouse pointer of your host operating system when the mouse pointer exits the virtual machine console window. This does not apply in full screen mode. Use this option to transition seamlessly between the virtual machine and your host operating system.
- **Hide cursor on ungrab** — the mouse pointer of the guest operating system is hidden when your mouse is controlling the pointer of the host operating system. This option is particularly useful when your guest operating system and your host operating system are identical: it eliminates the confusion of having to think about which of these two identical pointers will move if you move your mouse.
- **Scroll when cursor approaches window edge** — if your virtual machine's display area is larger than the GSX Server console window that displays it, then the console window only displays a part of your virtual screen. You can use scrollbars to scroll through the virtual machine's screen and see other areas of it. When this option is enabled and the virtual machine is not in full screen mode, the GSX Server virtual screen automatically scrolls the console window when the mouse pointer nears the edge of the viewable portion of the virtual screen. This option is useful since it avoids tedious "release focus, use scrollbars, capture focus" sequences.

  Note: This option is always temporarily enabled if you press a mouse button while moving the mouse. This allows you to perform easily tasks like selecting a group of objects, or dragging and dropping inside the virtual machine.
- **Enable copy and paste to and from virtual machine** — for copying and pasting text between the host and the virtual machine and among virtual machines. The clipboards of the two operating systems communicate with each other. When the mouse pointer of your guest operating system exits the console window, the contents of the guest operating system clipboard is copied into the host operating system clipboard. Similarly, each time the mouse pointer of your host operating system is grabbed by the console window, the contents of the host operating system clipboard is copied into the guest operating system

clipboard. You can disable the ability to copy and paste to and from virtual machines.

Note: At this time, you cannot copy and paste between Red Hat Linux 7.0 through 7.3 and Windows 2000. It does not matter which operating system is the guest and which is the host.

Setting Hot-Key Preferences

The GSX Server local and remote consoles contain a hot-key preferences editor where you can substitute an alternate hot-key combination (use of Ctrl, Alt and Shift keys in combination with other keys) if the default Ctrl+Alt combination conflicts with another application on the host that processes the same hot-key combination. These key combinations determine whether certain combinations of keys are passed to the guest operating system or intercepted by GSX Server.

Using the hot-key preferences editor, you can also construct your own custom hot key combination.

For example, you may want to change hot key combinations from Ctrl-Alt-<key> to Ctrl-Shift-Alt-<key> to prevent Ctrl-Alt-Delete from being intercepted by GSX Server instead of being sent to the guest operating system.

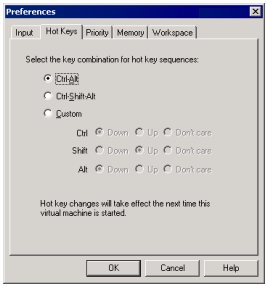
As another example, you are using PC Anywhere to connect to a machine running a local console. The virtual machine to which the local console is connected is in full screen mode, and you want to run a different application. Normally, to return to window mode, you would press Ctrl-Alt, but PC Anywhere processes Ctrl-Alt key combinations, so GSX Server cannot receive the key combination. Thus, you would need to use an alternate hot-key combination to get out of full screen mode.

Note: Because Ctrl-Alt is the key combination used to tell GSX Server to release (ungrab) mouse and keyboard input, combinations that include Ctrl-Alt are not passed to the guest operating system. If you need to use such a combination — for example, use Ctrl-Alt-<Fkey> to switch between Linux workspaces in a virtual machine — press Ctrl-Alt-Space, release Space without releasing Ctrl and Alt, then press the third key of the key combination you want to send to the guest.

Note: Changing the hot-key combination changes the sequence you need to use. For example, if you change the hot-key combination to Ctrl-Shift-Alt, you must press Ctrl-Shift-Alt-Insert to end the guest operating system session, and Ctrl-Shift-Alt to release the mouse and keyboard from the virtual machine to the host operating system.

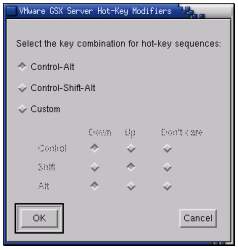
Accessing the Hot-Key Preferences Editor in a Windows Console

To set hot key preferences, in the Preferences dialog box, click the **Hot Keys** tab.



Accessing the Hot-Key Preferences Editor in a Linux Console

In the console window, choose **Settings** > **Hot-Key Modifiers**. The GSX Server Hot-Key Modifiers dialog box appears.



Setting Your Hot-Key Preferences

You can set your GSX Server hot-key combination to be the default (Ctrl-Alt), Ctrl-Shift-Alt or a combination you specify here. Select the appropriate radio button. If you select **Custom**, you need to specify the combination of Ctrl, Shift and Alt keys to use as the alternate sequence. You can set each key to be Down, Up or Don't Care.

If you select Down, then that key must be pressed down in a hot-key sequence. If you select Up, then that key must not be pressed in a hot-key sequence. If you select Don't Care, then you have the option of pressing the key.

On keyboards with both left and right Ctrl, Shift or Alt keys, pressing either key is acceptable for a Down-enabled key.

For example, if you select:

Control -> Down
Shift -> Up
Alt -> Down

Then you must press Ctrl-Alt to exit full screen mode (or use Ctrl-Alt with any other hot-key sequence); either the left or right Ctrl key (or both) must be pressed down, and either the left or right Alt key (or both) must be pressed down, and both of the Shift keys must be up (not pressed down).

As another example, if you select:

Control -> Down
Shift -> Down
Alt -> Don't Care

Then you can press Ctrl-Shift to exit full screen mode; the Ctrl and Shift keys must be pressed as in the previous example, but either Alt key may be or may not be pressed down.

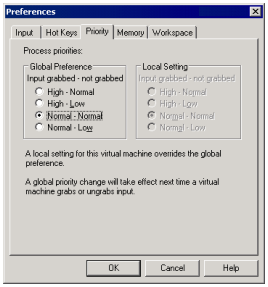
Setting Priority Preferences

GSX Server for Windows gives you the option to set the priority that the Windows process scheduler gives to your virtual machines when mouse and keyboard input are going to a particular virtual machine and when input is not going to that virtual machine. The priority settings here are used by all virtual machines unless a virtual machine configuration overrides the global setting with a local setting.

You can adjust these settings to improve overall system performance based on the relative priority of work you are doing in various virtual machines and on the host computer.

There is no corresponding setting on a Linux host.

To set priority preferences, in the Preferences dialog box, click the **Priority** tab.



There are three possible process scheduling priorities: low, normal and high. The typical process on the host runs at normal priority. If you set the priority of the virtual machine to low, the virtual machine has lower priority than other processes on the host. If you set the priority of the virtual machine to normal, the virtual machine contends with all the processes on the host. If you set the virtual machine priority to high, the virtual machine gets priority over other processes on the host.

GSX Server gives you the option to automatically change the process scheduling priority that applies when the virtual machine grabs and ungrabs keyboard and mouse input. For more information on grabbing and ungrabbing input, see Setting Input Preferences on page 207.

The four possible process priorities are

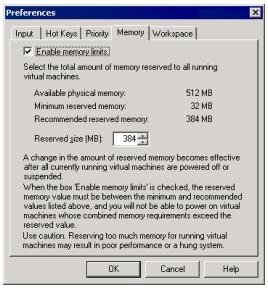
- **High - Normal:** When input is grabbed, GSX Server gets priority over other processes on the host. When input is not grabbed, GSX Server contends with all the processes on the host.
- **High - Low:** When input is grabbed, GSX Server gets priority over other processes on the host. When input is not grabbed, GSX Server has lower priority than other processes on the host.
- **Normal - Normal:** When input is grabbed, GSX Server contends with all the processes on the host. When input is not grabbed, GSX Server contends with all the processes on the host.
- **Normal - Low:** When input is grabbed, GSX Server contends with all the processes on the host. When input is not grabbed, GSX Server has lower priority than other processes on the host.

GSX Server defaults to process priority Normal - Normal.

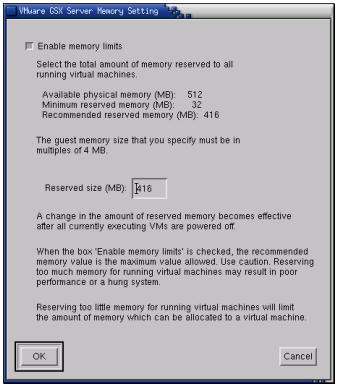
Process priority changes made under **Local Setting** affect this virtual machine and take effect immediately. Process priority changes made under **Global Preference** affect this virtual machine immediately (if there is not a local setting). Other running virtual machines, which do not override the global priority settings with a local setting, pick up the new global settings the next time input is grabbed or ungrabbed.

Setting Memory Preferences

To adjust the amount of memory reserved for all running virtual machines, on a Windows host in the Preferences dialog box, click the **Memory** tab.


Preferences
Input
Hot Keys
Priority
Memory
Workspace
Enable memory limits
Select the total amount of memory reserved to all running virtual machines.
Available physical memory: 512 MB
Minimum reserved memory: 32 MB
Recommended reserved memory: 384 MB
Reserved size (MB): 384
A change in the amount of reserved memory becomes effective after all currently running virtual machines are powered off or suspended.
When the box 'Enable memory limits' is checked, the reserved memory value must be between the minimum and recommended values listed above, and you will not be able to power on virtual machines whose combined memory requirements exceed the reserved value.
Use caution. Reserving too much memory for running virtual machines may result in poor performance or a hung system.
OK
Cancel
Help

On a Linux host, choose **Settings** > **Reserved Memory**. A dialog box allows you to adjust the amount of memory reserved to all running virtual machines.


VMware GSX Server Memory Setting
Enable memory limits
Select the total amount of memory reserved to all running virtual machines.
Available physical memory (MB): 512
Minimum reserved memory (MB): 32
Recommended reserved memory (MB): 416
The guest memory size that you specify must be in multiples of 4 MB.
Reserved size (MB): 416
A change in the amount of reserved memory becomes effective after all currently executing VMs are powered off.
When the box 'Enable memory limits' is checked, the recommended memory value is the maximum value allowed. Use caution. Reserving too much memory for running virtual machines may result in poor performance or a hung system.
Reserving too little memory for running virtual machines will limit the amount of memory which can be allocated to a virtual machine.
OK
Cancel

Virtual machines require relatively large amounts of memory to operate with reasonable performance. This memory comes out of the same pool of memory used by all applications on the host machine. The memory used by GSX Server includes the memory for the virtual machine itself as well as overhead memory associated with running a virtual machine. The virtual machine's memory size is specified in the virtual machine configuration.

GSX Server reserves the host's physical memory to improve virtual machine performance. This is done by locking physical memory. The amount of physical memory that is actually locked for a particular virtual machine varies dynamically as it

runs. If several virtual machines run simultaneously, they work together to manage the locked memory.

To provide good overall system performance, GSX Server limits the amount of the host's memory that can be locked by all virtual machines together. Any reserved memory used by virtual machines is not available to the other applications or to the host operating system. GSX Server uses the reserved memory only if it determines that a virtual machine needs reserved memory to have reasonable performance. Even if multiple virtual machines are running at the same time, GSX Server may be using only a fraction of the reserved memory, thus allowing any unused reserved memory to be used by other applications. Within this reserved memory pool an individual virtual machine can use at most the amount of memory configured in its configuration file plus some overhead. The amount of overhead memory required depends upon the size of the guest's virtual disks, its behavior and the amount of memory allocated to the virtual machine. Refer to the table below for the typical upper limit needed, based on the amount of memory allocated to the guest.

Amount of Memory Allocated to the Virtual Machine	Additional Amount of Overhead Needed
Up to 512MB	Up to 40MB
Up to 1GB	Up to 50MB
Up to 2GB	Up to 70MB

GSX Server allows you to set the maximum amount of memory to reserve. The recommended amount of memory to reserve for GSX Server applications is 50% of the host's physical memory. If you determine that you want GSX Server to reserve more or less physical memory, you can change this amount by changing the value in Reserved size (MB). Changing the amount of reserved memory is recommended only for advanced users because it can have an adverse impact on host or virtual machine performance. Selecting to reserve too much physical memory can cause the host to thrash, or even hang, if other applications are run on the host. Selecting to reserve too little physical memory can cause virtual machines to perform very poorly and also limit the number of virtual machines that can be run.

By default, a virtual machine performs two checks to ensure that enough free memory is left to the host machine to continue to operate efficiently. First, at power on, it checks that the total amount of memory allocated to all running virtual machines does not exceed the total physical memory of the host. Second, the virtual machine periodically checks that the reserved memory allocated to currently running

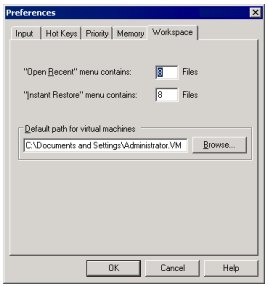
virtual machines does not exceed the total amount of reserved memory. If the first check fails, the virtual machine does not power on; if the second check fails, GSX Server attempts to compensate by reducing the virtual machine's memory use.

If you want to disable this check on memory limits, see Disabling Memory Checks for Virtual Machines on page 531.

For more information about memory and virtual machines, see Understanding Memory on page 529.

Setting Workspace Preferences

To set workspace preferences, on a Windows host, in the Preferences dialog box, click the **Workspace** tab.



The settings you can specify here include:

- How many virtual machines are shown in the recently used virtual machines submenu in a local console. The number specified in the **Open Recent menu contains** field limits the number of entries you see when you choose **File** > **Open Recent** in a local console.
- How many virtual machines are shown in the instant restore submenu in a local console. The number specified in the **Instant Restore menu contains** field limits the number of entries you see when you choose **File** > **Instant Restore** in a local console.
- The default folder where virtual machine files are placed when you create new virtual machines.

There are no corresponding settings on a Linux host.

Closing a Console

When you are finished running a remote console, you can close the console window without shutting down the guest operating system. On a Windows host, click **Detach and Close** on the remote console toolbar to close the console. On a Linux host, choose **File** > **Exit**. This does not affect the guest operating system in any way. The virtual machine keeps running.

If you are running a local console, you must suspend or shut down the guest operating system before you close the local console window. This allows other users to access the virtual machine.

8

Running Virtual Machines

A Quick Guide to Running VMware GSX Server Virtual Machines

Now that you have installed GSX Server, a guest operating system and VMware Tools, how do you run your virtual machine? The following show various features of the product and highlight the most common tasks:

- Displaying Hints on page 220
- Checking the Status of VMware Tools on page 221
- Using Full Screen Mode on page 222
- Installing New Software Inside the Virtual Machine on page 222
- Cutting, Copying and Pasting on page 223
- Sharing Files Between Guest and Host Operating Systems on page 223
- Deciding How Your Virtual Machine Stores Data on page 228
- Suspending and Resuming Virtual Machines on page 229
- Resuming Virtual Machines Repeatedly from the Same Point on page 231
- Shutting Down a Virtual Machine on page 235
- Running Virtual Machines from DVD-ROM or CD-ROM Discs on page 235
- Adding, Configuring and Removing Devices in a Virtual Machine on page 237
- Connecting and Disconnecting Removable Devices on page 239
- Fitting the GSX Server Console Window to the Virtual Machine on page 239
- Creating a Screen Shot of a Virtual Machine on page 239
- Command Reference on page 240

Displaying Hints

GSX Server can display hints that appear in response to various actions you take when running a virtual machine. The hints provide more information about these actions. By default, hints are turned off. If you want hints to appear, in a console, choose **Settings** > **Show All Hints**. VMware recommends that users new to GSX Server should display hints.

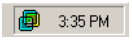
Each hint can be hidden on a case by case basis. When you want to hide a hint, check **Never show this hint again** before dismissing the hint dialog box.

Caution: On a Linux host, if hints are enabled, a virtual machine cannot enter full screen mode when you click the **Full Screen** button on the toolbar in the local console. In order to put the virtual machine into full screen mode, use the Ctrl-Alt-Enter key combination or choose **View** > **Full Screen**.

Checking the Status of VMware Tools

For best performance, it is important to have VMware Tools installed and running in your virtual machine. For more information about VMware Tools, see Using VMware Tools on page 109.

After you install VMware Tools in a Windows virtual machine, VMware Tools starts automatically when you start the guest operating system.



When VMware Tools is running in a Windows virtual machine, the VMware Tools icon appears in the system tray unless you disable the icon.

If the VMware Tools icon is not displayed in the system tray, you can use the VMware Tools control panel in the guest operating system (**Start** > **Settings** > **Control Panel**) to change settings for VMware Tools. You can also reactivate the system tray icon. On the **Options** tab, check the **Show VMware Tools in the task bar** check box.

In a Linux or FreeBSD virtual machine, boot the guest operating system, start X and launch your graphical environment. Then you can launch the VMware Tools background application with this command:

```
vmware-toolbox &
```

You may run VMware Tools as root or as a normal user. To shrink virtual disks, you should run VMware Tools as root (`su -`), to maximize the shrink's effectiveness. To test and edit scripts, you must run VMware Tools as the root user.

In a NetWare 5.1 or 6.0 guest operating system, you can access the VMware Tools control panel by choosing **Novell** > **Settings** > **VMware Tools for NetWare**.

With some window managers, you can place the command to start VMware Tools in a startup configuration so VMware Tools starts automatically when you start your graphical environment. For more information, see Starting VMware Tools Automatically on page 118.

Using Full Screen Mode

Full screen mode is available only when using the local console on the server, that is, when you launch the console on a Windows host by selecting **Start** > **Programs** > **VMware** > **VMware GSX Server** (or, double-click the VMware GSX Server icon on your desktop); on a Linux host, you launch the console with this command: `vmware -G`.

You run the local console when you need exclusive access to a virtual machine, for example, when you are installing the virtual machine's guest operating system and VMware Tools. Virtual machines run faster in full screen mode.

If you want your GSX Server virtual machine's display to fill the screen — so you no longer see the borders of the GSX Server local console window — click the **Full Screen** button on the toolbar. You can also use a keyboard shortcut — press the Ctrl-Alt-Enter keys at the same time.

To get out of full screen mode — to show your virtual machine inside a GSX Server local console window again — press the Ctrl-Alt key combination.

You can switch between virtual machines without leaving full screen mode by using a Ctrl-Alt-Fn key combination, where Fn is a function key corresponding to the virtual machine you want to see. To find out what function key to use for a particular virtual machine, check the title bar of the virtual machine while it is running in a console window.

Note: GSX Server does not support running virtual machines in full screen mode on dual-monitor systems.

Caution: On a Linux host, if hints are enabled, a virtual machine cannot enter full screen mode when you click the **Full Screen** button on the toolbar in the local console. In order to put the virtual machine into full screen mode, use the Ctrl-Alt-Enter key combination or choose **View** > **Full Screen**.

Installing New Software Inside the Virtual Machine

Installing new software in a GSX Server virtual machine is just like installing it on a physical computer. These steps assume you are installing software inside a Windows 2000 guest operating system.

1. Be sure you have started the virtual machine and, if necessary, logged on. Check the **Devices** menu to be sure the virtual machine has access to the CD-ROM drive and, if needed, the floppy drive.
2. Insert the installation CD-ROM or floppy disk into the proper drive on the GSX Server host. If you are installing from a CD-ROM, the installation program may start automatically.

3. If the installation program does not start automatically, click the Windows **Start** button, go to **Settings** > **Control Panel**, then double-click **Add/Remove Programs** and click the Install button. Follow the instructions on screen and in the user manual for your new software.

Note: Some applications use a product activation feature that creates a key based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine may require you to reactivate the software. To minimize the number of significant changes, set the final memory size for your virtual machine and install VMware Tools before you activate the software.

Cutting, Copying and Pasting

When VMware Tools is running, you can cut or copy then paste text between applications in the virtual machine and the host computer or between two virtual machines. Use the normal hot keys or menu choices to cut, copy and paste.

Note: If you are copying text from a Windows host into a Linux guest operating system, you can paste only by using the middle mouse button. If you are using a two-button mouse, click both mouse buttons at the same time to paste.

To turn off this feature — to prevent accidental copying and pasting from one environment to another — use the **Settings** menu.

On a Windows host, choose **Settings** > **Preferences**. On the **Input** tab, clear the **Enable copy and paste to and from virtual machine** check box.

On a Linux host, choose **Settings** > **Input Preferences**. On the cascading menu, check to see whether there is an activated icon next to **Allow copy and paste to and from virtual machine**. If there is, click **Allow copy and paste to and from virtual machine** to turn off the feature.

Sharing Files Between Guest and Host Operating Systems

To share files between a host computer and a virtual machine or between two virtual machines, you use the networking features of GSX Server. If you know how to share files between two physical computers on a network, you already know how to share files with a virtual machine.

This section describes four scenarios for sharing files between two systems, either a host computer and a virtual machine or two virtual machines, where

- Both systems run Windows operating systems, using Windows file sharing
- You are connecting from a Linux system to a Windows system, using `smbmount`

- You are connecting from a Windows system to a Linux system, using Samba
- Both systems run Linux operating systems, using NFS, FTP and Telnet

You can apply the same principles to share files between virtual machines.

The following scenarios assume you have set up your virtual machine using NAT networking. Besides giving the virtual machine a direct connection to the host computer's network, NAT networking sets up a virtual network adapter on the host computer. You can use this adapter, which connects to a virtual switch identified as `vmnet8`, to communicate between host and virtual machine. You can also connect two or more virtual machines using `vmnet8`. For details on NAT networking, see Network Address Translation (NAT) on page 409.

In all cases, the user name you used to log in to the system from which you are connecting must be a user on the system to which you want to connect.

Sharing Files Between Two Windows Systems

To share files between two Windows systems (where one machine is a host and the other is a virtual machine, or both are virtual machines), be sure the file and printer sharing service is installed for both operating systems and the folders you want to share are marked as shared. Then you can browse from one system to the shared folder or folders on the other system.

Sharing Files by Connecting to a Windows System from a Linux System

To share files on a Windows system with a Linux system (by connecting to a Windows host from a Linux guest or connecting to a Windows guest from a Linux host or guest), you can mark a folder as shared on the Windows system, then use the `smbmount` utility in the Linux system to mount the shared folder. For example, if you want to share the folder `C:\docs` on a Windows 2000 system called `win2k` with a Linux system at `/mnt/docs`, follow the steps below. You may want to set up a shell script to run these commands.

1. Set up the folder or folders to share on the Windows system.
2. Create a user account on the Windows system for the Linux system user name that you are using to connect to the Windows system.

   Otherwise, if you know the user name and password for a user account that can access the Windows system, you can specify that account on the command line.
3. From your Linux system, log in as root.

   ```
   su -
   ```
4. Add the Windows system's host name and IP address to the `hosts` file, if the system cannot be found by name.

5. Mount the Windows share on your Linux system. Enter the following command all on one line.

   ```
   mount -t smbfs -o username=<Windows system user
   account>,password=<password> //win2k/docs /mnt/docs
   ```

   (Substitute the appropriate host name, share and mount point for your systems.)

Note: If you do not want to expose this password on the command line or in a script, leave out that option and provide the password when prompted after you run the command.

Now you are connected to the shared folder on the Windows system from your Linux system and can begin to share files between the two.

Sharing Files by Connecting to a Linux System from a Windows System

To share files on a Linux system with a Windows system (by connecting to a Linux host from a Windows guest or connecting to a Linux guest from a Windows host or guest), you can run Samba on the Linux system and browse shared directories in the Linux file system from Network Neighborhood in the Windows system.

You need to modify Samba on the Linux host operating system so it recognizes the `vmnet8` switch, otherwise you cannot access the Linux file system. You need to do this even if you installed host-only networking (as Samba is installed when you install host-only networking with GSX Server). For more information about Samba, see Using Samba for File Sharing on a Linux Host on page 431.

Connecting to a Linux Host from a Windows Guest

If you want to share the directory `/home/user/shared`, for example, on a Linux host operating system with a Windows guest operating system, follow these steps:

1. On the Linux host operating system, back up the `smb.conf` file to a file called something like `smb.conf.orig`.

   ```
   cd /etc/vmware/vmnet1/smb
   cp smb.conf smb.conf.orig
   ```

2. Modify Samba on the Linux host system. Edit the following lines in `/etc/vmware/vmnet1/smb/smb.conf`.

   A. Comment out the line starting with `interfaces=<IP addresses>`.

   B. Below this line, add `interfaces=vmnet1 vmnet8`.

   C. Provide a network workgroup name. Set `workgroup=<name>`.

   D. If you do not want to use the standard DNS name for the Linux system, set `netbiosname=<Linux system name>`.

E. You can leave `security=user`, unless you cannot connect, in which case use `security=share`.

F. Set `encrypt passwords=yes`.

G. In the `[global]` section, define a different shared memory access key. Add this line:
```
sysv shm key=/dev/vmnet8
```

H. For better performance, at this line:
```
socket options = TCP_NODELAY
```
edit the line to state:
```
socket options = TCP_NODELAY SO_RCVBUF=8192
SO_SNDBUF=8192
```
Note: This setting must be entered on one line.

I. To create the share, add the following:
```
[SHARE_NAME]
path = /home/user/shared
public = no
writable = yes
printable = no
```
(since you want to share files, not a printer)

J. Save this file and create a backup copy to protect these changes when you upgrade GSX Server.

3. Restart the Samba services to load the new settings.

   If GSX Server is running on the Linux host system, suspend or shut down all running virtual machines and close all GSX Server console windows.

   On the Linux host operating system, at a command prompt, type

   ```
   /etc/init.d/vmware restart
   ```

   On some Linux distributions, the command is

   ```
   /etc/rc.d/init.d/vmware restart
   ```

   Connect to the virtual machine with a console and run the Windows guest operating system from which you want to connect to the Linux host. The user ID you use to log in to the Windows guest must be in the Linux host's `smbpasswd` file. If you use the same user name and password to log in to the guest as you do on the Linux host, then you are not prompted to log in when you browse the Linux host.

   If you are connecting to the Linux system from a Windows Me, Windows 98 or Windows 95 guest operating system, NetBEUI must be installed in the guest

operating system before you can browse the file system. If you need to install NetBEUI, you may need your Windows installation CD-ROM.

When the system restarts, the Samba service does not appear in the list of services starting up, but it does start, unless an error appears.

Connecting to a Linux Guest from a Windows Host or Guest

To share the directory `/home/user/shared`, for example, on a Linux guest operating system with a Windows host or guest operating system, follow these steps:

1. On the Linux guest operating system, back up the `smb.conf` file to a file called something like `smb.conf.orig`.
   `cp /etc/smb.conf /etc/smb.conf.orig`
2. Modify Samba on the Linux system to share the directory. To create the share, add the following to `/etc/smb.conf`.

   ```
   [SHARE_NAME]
   path = /home/user/shared
   public = no
   writable = yes
   printable = no
   ```
   (since you want to share files, not a printer)
3. Restart the Samba services to load the new settings. On the Linux guest operating system, at a command prompt, type:

   `/etc/init.d/smb restart`

   On some Linux distributions, the command is

   `/etc/rc.d/init.d/smb restart`

   When the system restarts, the Samba service appears in the list of services starting up.

Sharing Files Between Two Linux Systems

To share files between two Linux systems (where one machine is a host and the other is a virtual machine, or both are virtual machines), you can use NFS on the system to connect to and the `nfsmount` utility in the system from which you are making the connection.

As with any Linux network, you can use NFS, FTP or Telnet to connect from one Linux system (either virtual or physical) to another Linux system (either virtual or physical).

Deciding How Your Virtual Machine Stores Data

Do you ever have a bad day and wish you could get rid of all the changes you've made to files on your computer? In a GSX Server virtual machine, you can. The secret is in the disk modes.

GSX Server uses disks in three different modes — persistent, undoable and nonpersistent.

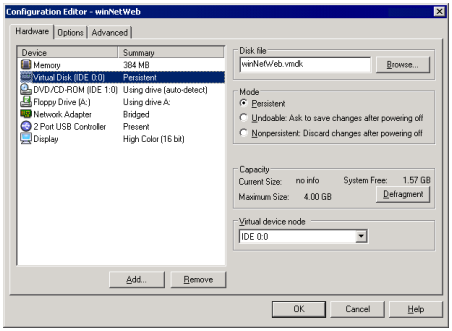
Disks in persistent mode behave exactly like conventional disk drives on a computer. All data written to a disk in persistent mode is written out permanently to the disk as soon as the guest operating system writes the data.

When you use undoable mode, you have the option later of keeping or discarding changes you have made while the virtual machine is running. Until you decide, the changes are saved in a redo-log file. You can also keep the changes for the next time the virtual machine runs, but still have the option of discarding all the accumulated changes at some time in the future.

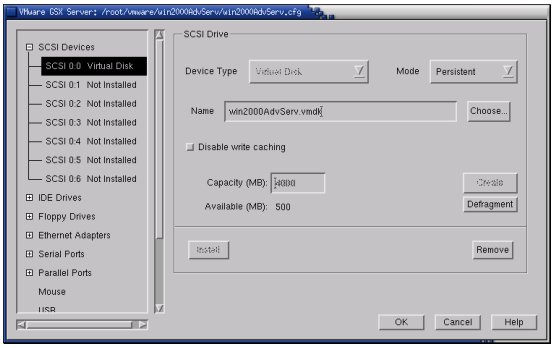
All changes to a disk in nonpersistent mode are discarded after the virtual machine is powered off.

You can use the Configuration Editor to change the disk mode for your virtual machine.

1. Connect to the virtual machine from a console, but don't click the **Power On** button yet. For information, see Connecting to Virtual Machines from Local and Remote Consoles on page 187.
2. Choose **Settings** > **Configuration Editor**. The Configuration Editor appears.
3. On a Windows host, click the name of the drive you want to change.



On a Linux host, click the + sign beside **IDE Drives** or **SCSI Drives** to expand that part of the tree, then click the name of the drive you want to change.



4. Select the appropriate option for persistent, undoable or nonpersistent mode.

   Click **OK** to save your changes and close the Configuration Editor.

Suspending and Resuming Virtual Machines

You can save the current state of your virtual machine by suspending it. Then you can resume the virtual machine to pick up work quickly, right where you stopped — with all documents you were working on open and all applications in the same state as they were at the time you suspended the virtual machine.

The speed of the suspend and resume operations depends on how much data has changed while the virtual machine has been running. In general, the first suspend operation takes a bit longer than later suspend operations do.

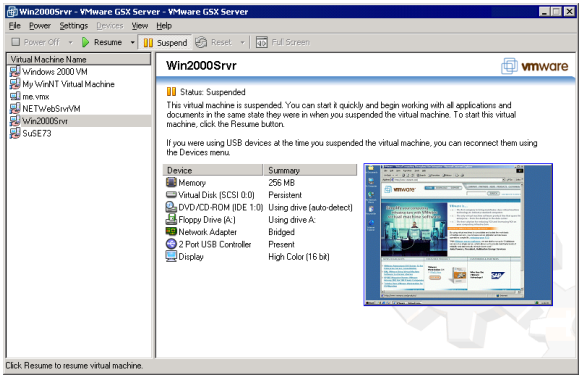
When you suspend a virtual machine, a file with a `.vmss` extension is created. This file contains the entire state of the virtual machine. When you resume the virtual machine, its state is restored from the `.vmss` file. The `.vmss` file cannot be used to resume a virtual machine again from the original suspended state.

This behavior ensures that a `.vmss` file is used only once to resume a virtual machine — which is the safest behavior. Note that a virtual machine you have suspended and resumed may be suspended again, appending to the `.vmss` file.

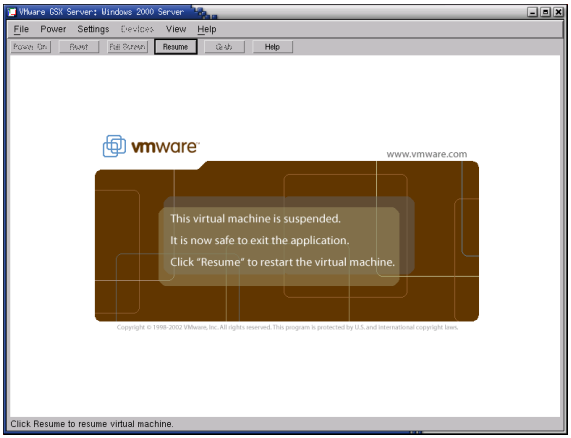
When you suspend a virtual machine in a local console, you must resume it in a local console. Similarly, if you suspend a virtual machine in the VMware Remote Console, you must resume it in a remote console.

To suspend a virtual machine:

1. If your virtual machine is running in full screen mode, return to window mode by pressing the Ctrl-Alt key combination.
2. Click **Suspend** on the console toolbar.


Win2000Srvr - VMware GSX Server - VMware GSX Server
File Power Settings Devices View Help
Power Off Resume Suspend Reset Full Screen
Virtual Machine Name
Windows 2000 VM
My WinNT Virtual Machine
me.vmx
NETWebSrvVM
Win2000Srvr
SuSE73
Win2000Srvr
vmware
Status: Suspended
This virtual machine is suspended. You can start it quickly and begin working with all applications and documents in the same state they were in when you suspended the virtual machine. To start this virtual machine, click the Resume button.
If you were using USB devices at the time you suspended the virtual machine, you can reconnect them using the Devices menu.
Device Summary
Memory 256 MB
Virtual Disk (SCSI 0:0) Persistent
DVD/CD-ROM (IDE 1:0) Using drive (auto-detect)
Floppy Drive (A:) Using drive A:
Network Adapter Bridged
2 Port USB Controller Present
Display High Color (16 bit)
Click Resume to resume virtual machine.

VMware GSX Server on a Windows host with a suspended virtual machine


VMware GSX Server: Windows 2000 Server
File Power Settings Devices View Help
Power On Reset Full Screen Resume Grab Help
vmware
www.vmware.com
This virtual machine is suspended.
It is now safe to exit the application.
Click "Resume" to restart the virtual machine.
Click Resume to resume virtual machine.

VMware GSX Server on a Linux host with a suspended virtual machine

3. When GSX Server has completed the suspend operation, you see a screen similar to one of those above, depending on your host operating system. It is safe to close the console.

   File > **Exit**

To resume a virtual machine that you have suspended:

1. Start a console and choose a virtual machine you have suspended. The process is the same as that described in Connecting to Virtual Machines from Local and Remote Consoles on page 187.

   If you suspended a virtual machine in a local console, you must resume it in a local console. If you suspended a virtual machine in the VMware Remote Console, you must resume it in a remote console.

2. Click **Resume** on the console toolbar.

   Note that any applications you were running at the time you suspended the virtual machine are running and the content is the same as it was when you suspended the virtual machine.

Resuming Virtual Machines Repeatedly from the Same Point

When you suspend a virtual machine in the usual way, by clicking the **Suspend** button on the console toolbar or in the management interface, a file with a `.vmss` extension is created. This file contains the entire state of the virtual machine. When the virtual machine is resumed, its state is restored from the `.vmss` file. This means that, in normal operation, the `.vmss` file cannot be used to resume a virtual machine again from the original suspended state.

If you want to be able to resume a virtual machine in the same state repeatedly — for example, in a QA testing or classroom environment — then you can take advantage of repeatable resume. Every time you resume the virtual machine, it starts from the same point at which it was suspended using the same `.vmss` file. This feature works only with virtual disks in nonpersistent mode. For a discussion of disk modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 368.

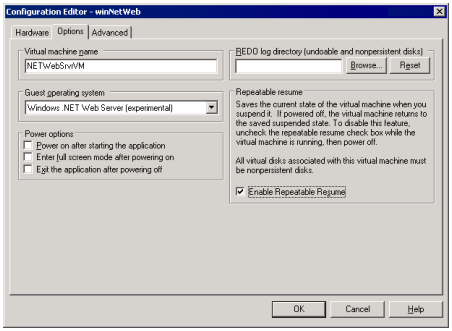
Repeatable resume makes it easy to start a virtual machine again and again in the exact same state. However you cannot suspend this virtual machine; you can only power it off. After you power it off, you can resume the virtual machine to start it up again. The virtual machine starts at the point at which it was suspended.

If you need to reset a virtual machine that is set up to use repeatable resume, you should restart the guest operating system (using **Start** > **Shut Down** > **Restart** for Windows guests, `shutdown -r now` for Linux guests). Do not click the **Reset** button on the virtual machine's toolbar. Otherwise, any files you created or other changes made to the guest operating system are lost.

Restarting or resetting the guest operating system does not affect the suspended state. To return to your repeatable resume point, just power off the virtual machine, then resume it.

Enabling Repeatable Resume on a Windows Host

1. Make sure the virtual machine is powered off. You can enable the repeatable resume feature only when the virtual machine is powered off.
2. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
3. All virtual disks associated with this virtual machine must be in nonpersistent mode before you can enable repeatable resume. In the Configuration Editor, on the **Hardware** tab, select the virtual disk. Under **Mode**, make sure the **Nonpersistent** radio button is selected.
4. Click the **Options** tab.

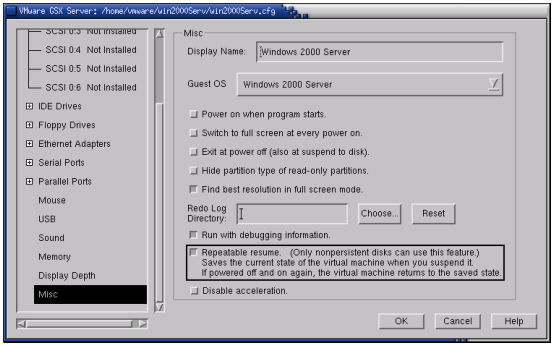

Configuration Editor - winNetWeb
Hardware
Options
Advanced
Virtual machine name
NETWebSrvVM
REDO log directory (undoable and nonpersistent disks)
Browse...
Reset
Guest operating system
Windows .NET Web Server (experimental)
Repeatable resume
Saves the current state of the virtual machine when you suspend it. If powered off, the virtual machine returns to the saved suspended state. To disable this feature, uncheck the repeatable resume check box while the virtual machine is running, then power off.
All virtual disks associated with this virtual machine must be nonpersistent disks.
Power options
Power on after starting the application
Enter full screen mode after powering on
Exit the application after powering off
Enable Repeatable Resume
OK
Cancel
Help

5. If you intend to copy this virtual machine to other PCs, VMware suggests that you locate the redo log in the same directory as the virtual machine. Click **Browse** to find the virtual machine's directory and select it. For more information about the location of the redo log, see Configuration Parameters to Consider on page 233.
6. Check the **Enable Repeatable Resume** check box.
7. Click **OK** to save your changes and close the Configuration Editor.

Enabling Repeatable Resume on a Linux Host

1. Make sure the virtual machine is powered off. You can enable the repeatable resume feature only when the virtual machine is powered off.
2. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
3. All virtual disks associated with this virtual machine must be in nonpersistent mode before you can enable repeatable resume. In the Configuration Editor, under **SCSI Devices** or **IDE Drives**, select the virtual disks and make sure the **Mode** is set to **Nonpersistent**.

4. Click **Misc**. The **Misc** panel appears.



5. If you intend to copy this virtual machine to other PCs, VMware suggests that you locate the redo log in the same directory as the virtual machine. Click **Choose** to find the virtual machine's directory and select it. For more information about the location of the redo log, see Configuration Parameters to Consider on page 233.
6. Select **Repeatable resume**.
7. Click **OK** to save your changes and close the Configuration Editor.

Configuration Parameters to Consider

Caution: By default, the redo-log file for a disk in nonpersistent mode is located in your system's temp directory. If you intend to move this virtual machine to another host, VMware suggests that you place the redo log for a virtual machine using repeatable resume in a different location (outlined in the steps below), as some temp directories may be small (and the redo log could exceed this limit as it grows) or, on Linux hosts, the temp directory may be cleared by the operating system on a regular basis, and this would remove the redo log.

Caution: VMware does not recommend moving a suspended virtual machine containing disks in nonpersistent mode to another host. However, if you want to take advantage of the repeatable resume feature in a classroom environment, for example, and do not want to set the same repeatable resume point individually on every student's machine, be very careful and keep the following warnings in mind:

- VMware does not support the use of repeatable resume with a virtual machine when its disks are located on a networked drive. However, if you place a disk in nonpersistent mode on a shared network drive, note that locating the redo log

in a directory on a networked drive may affect the performance of your virtual machine.

- Do not distribute the virtual disk (`.vmdk`) files. Place the virtual disks in a location on a shared network drive the whole class can access. Multiple users can run the same nonpersistent disk at one time.
- Make sure all the machines in the classroom contain the same hardware as the machine on which the virtual disk resides. This reduces the chance of hardware inconsistencies when the student resumes the virtual machine.
- Before you power on the virtual machine and create your repeatable resume point, put the redo log in the directory with the virtual machine's configuration file. Use the Configuration Editor (choose **Settings** > **Configuration Editor**, then select the **Options** tab for Windows hosts, **Misc** panel for Linux hosts) to specify the location of the redo log.
- After you create your repeatable resume point, copy all the files from the directory containing the virtual machine's configuration file to each student's computer.

Note: VMware recommends that if your virtual machine has repeatable resume enabled and is configured for DHCP, you should have a short lease time on IP addresses.

Disabling Repeatable Resume

If you no longer want to resume the virtual machine from this repeatable resume point, do the following:

1. Resume the virtual machine, if it is not running already. The virtual machine must be running for you to disable the repeatable resume feature.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**). Then do one of the following:
   - On a Windows host, click the **Options** tab, then clear the **Enable Repeatable Resume** check box.
   - On a Linux host, click **Misc**, then deselect **Enable repeatable resume**.

   You may want to change the disk mode from nonpersistent to persistent or undoable.
3. Click **OK** to save your changes and close the Configuration Editor.
4. Power off the virtual machine. This removes the suspend state (`.vmss` file) and allows you to suspend and resume the virtual machine normally again. All redo-log files for this virtual machine are removed.

With the virtual machine powered off, you can enable the feature again so that the next time you power on, you can set the virtual machine into a different state and save that as a new repeatable resume point.

Shutting Down a Virtual Machine

As with physical computers, you need to shut down your guest operating system before you power off your virtual machine. In most Windows guest operating systems, take these steps.

1. Select **Shut Down** from the **Start** menu of the guest operating system (inside the virtual machine).
2. Select **Shut Down**, then click **OK**.
3. After the guest operating system shuts down, you can turn off the virtual machine. Click **Power Off**.
4. Now it is safe to close the console.

   File > **Exit**

If you are using a different guest operating system, the procedure is similar. Follow the usual steps to shut down the guest operating system inside your virtual machine, then turn off the virtual machine with the **Power Off** button and close the console.

Note: On a Windows host, if you inadvertently attempt to close the local console while the guest operating system is still running, a dialog box appears. It gives you the option of suspending the virtual machine before exiting.

Running Virtual Machines from DVD-ROM or CD-ROM Discs

You can store a virtual disk on DVD-ROM or CD-ROM, and run the virtual machine from your GSX Server host's DVD/CD-ROM drive. You do not have to copy the virtual disk files from the DVD-ROM or CD-ROM to the GSX Server host.

One suggested use for this method is if you installed GSX Server on a host you want to use for product demonstrations, which could be a laptop. Instead of taking up limited hard disk space with virtual disks, you can have any number of virtual machines with virtual disks burned onto DVD-ROM or CD-ROM and point each virtual machine's configuration file to the virtual disk on the DVD-ROM or CD-ROM.

Other uses include sales or proof-of-concept demonstrations where you want to keep virtual disk files off a customer's system but want to illustrate a multiple machine demonstration in the customer's environment. Or you can have multiple physical servers in a datacenter run virtual machines without copying the virtual disk files to the servers themselves. Yet another method is if you need a "master" virtual machine

for some purpose, you can create a write-protected copy of your original virtual machine.

The virtual disk must be in nonpersistent or undoable mode, since any changes you make in the virtual machine cannot be written to the DVD-ROM or CD-ROM. The redo log for the virtual machine must be on the GSX Server host. If you choose to put the virtual disk in undoable mode, and you want to commit the changes to the virtual disk, the virtual disk must be copied onto the GSX Server host's hard drive in order for you to commit the changes in the redo log to the virtual disk. Otherwise, you can keep appending changes to the redo log. For more information on disk modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 368.

In addition, consider whether you may need to modify the virtual machine's BIOS at some point. In this case, the virtual machine's BIOS, which is stored in a file called `nvram`, must be located on the GSX Server host. Otherwise, you can add a setting to the virtual machine's configuration file that allows for the `nvram` file to be on the DVD-ROM or CD-ROM, where it cannot be modified.

Note: The performance of the virtual machine accessing a virtual disk stored on a DVD-ROM or CD-ROM depends upon the speed of the DVD-ROM/CD-ROM drive. Keep in mind that a virtual machine on a DVD-ROM/CD-ROM drive runs slower than it would if it were running on your host's hard disk.

To run a virtual machine from DVD-ROM or CD-ROM, complete the following steps.

1. Create a virtual machine and install the guest operating system and any applications you need within it.
2. Make sure the virtual machine is powered off. Burn the virtual disk (`.vmdk`) files onto a DVD-ROM or CD-ROM. Place the DVD-ROM or CD-ROM into the GSX Server host's DVD-ROM or CD-ROM drive.
3. Choose **Settings** > **Configuration Editor** to open the Configuration Editor for this virtual machine. On the **Hardware** tab, select **Virtual Disk** and browse to the virtual disk file on the DVD-ROM or CD-ROM.

   Under **Mode**, set the disk mode to **Nonpersistent**.
4. On the **Options** tab, under **REDO log directory**, select a location for the redo log on the GSX Server host.
5. Click **OK** to save your changes. The Configuration Editor closes.
6. In a text editor, open the virtual machine's configuration file (`.vmx` on Windows hosts, `.cfg` on Linux hosts) and add the following lines to the file:

   ```
   disk.locking = FALSE
   ```

`nvram = <path on GSX Server host>\nvram` (if you think you need to modify the virtual machine's BIOS)
or
`nvram.mode = "nonpersistent"` (if you do not need to modify the virtual machine's BIOS)

7. Save your changes and close the configuration file.

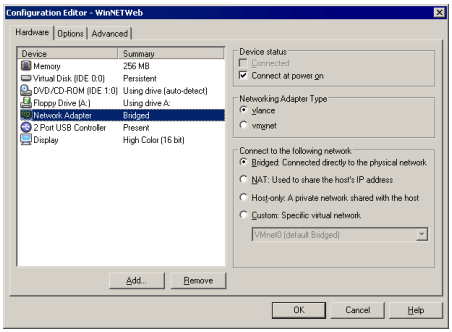
The virtual machine is now ready to be run from the GSX Server host's DVD/CD-ROM drive.

Note: Another method you can use is to burn all virtual machine files (the configuration file, `nvram` and virtual disk files) onto DVD-ROM or CD-ROM. First make sure the redo log directory points to a drive on your GSX Server host and that the configuration file has all the desired settings before you burn the files onto the DVD-ROM or CD-ROM.

Adding, Configuring and Removing Devices in a Virtual Machine

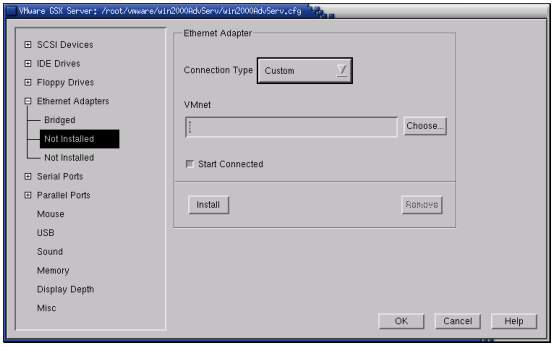
The Configuration Editor (**Settings** > **Configuration Editor**) is the control center where you can add devices to a virtual machine, change the settings for those devices and remove them.

To add a new device on a Windows host, open the Configuration Editor, click **Add**, then follow the instructions in the New Hardware Wizard to add the device to your virtual machine. Click **OK** to save your changes and close the Configuration Editor.



To add a new device on a Linux host, open the Configuration Editor, click the + sign beside the type of device you want to add, click a device that's shown as **Not Installed**

and make the appropriate settings. Click **Install** to install the device and **OK** to save your configuration changes and close the Configuration Editor.



To change settings for a device, open the Configuration Editor, select the device you want to modify and make your changes. Click **OK** to save your changes and close the Configuration Editor.

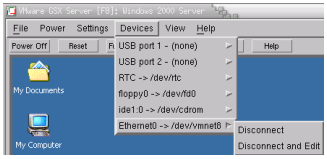
To remove a device, open the Configuration Editor, click the name of the device you want to remove, then click **Remove**. Click **OK** to close the Configuration Editor.

Connecting and Disconnecting Removable Devices

Use the **Devices** menu to connect and disconnect removable devices that you have configured for your virtual machine — including floppy drives, DVD/CD-ROM drives and USB devices — while the virtual machine is running.

On a Windows host, move the mouse pointer over a device name. A cascading menu gives you choices for connecting or disconnecting the device and, where appropriate, for editing the configuration settings for the device.

On a Linux host, click the device name. A cascading menu gives you choices for connecting or disconnecting the device and, where appropriate, for editing the configuration settings for the device.



Fitting the GSX Server Console Window to the Virtual Machine

The **View** menu gives you two ways to adjust the size of the GSX Server console window so it exactly fits the virtual machine's display.

Autofit is toggled on or off each time you click it. When **Autofit** is on, the console window adjusts automatically to fit the virtual machine's display. When it is off, you can adjust the console window to a size of your choice. If you make the console window smaller than the virtual machine's display, scroll bars appear so you can move to the part of the virtual machine's display that you want to see.

If **Autofit** is off, you can choose **View** > **Fit** to adjust the GSX Server console window so it fits the virtual machine's display.

Creating a Screen Shot of a Virtual Machine

In a Windows local console, you can capture a screen shot of a virtual machine. Choose **File** > **Capture Screen**. You save this image as a Windows bitmap (`.bmp`) file.

There is no corresponding function in a Linux local console.

Command Reference

Linux Host

The following list describes various options available when you run GSX Server from the command line on a Linux host operating system.

```
vmware [-x ] [-X ] [-q ]
[/<path_to_config>/<config>.cfg ]
[X toolkit options ]
```

`-x` automatically powers on the virtual machine when the local console launches. This is equivalent to clicking the **Power On** button on the console toolbar.

`-X` automatically powers on the virtual machine, then switches the GSX Server local console window to full screen mode.

`-q` exits the console when the virtual machine powers off. This is particularly useful when the guest operating system is capable of powering off the virtual machine.

`/<path_to_config>/<config>.cfg` launches a virtual machine using the specified configuration file.

X toolkit options can be passed as arguments, although some of them (most notably the size and title of the GSX Server console window) cannot be overridden.

Windows Host

The switches described above for Linux can also be used on a Windows host. The most convenient way to use the switches is to incorporate them into the command generated by a Windows shortcut.

Create the shortcut, right-click the shortcut, then click **Properties**. In the **Target** field, add any switches you want to use after the `vmware.exe` filename. For example,

```
"C:\Program Files\VMware\VMware GSX Server\Programs\vmware.exe -X
C:\Documents and Settings\<username>\My Documents\My Virtual
Machines\Windows 2000\Windows 2000.vmx"
```

launches the Windows 2000 virtual machine specified, powers it on automatically and switches to full screen mode.

Be sure to enclose the entire command string in quotation marks.

Note: On Windows, the configuration file has a `.vmx` extension by default. And path names on Windows use the backslash character (\). X toolkit options are not relevant on a Windows host.

9

Moving and Sharing Virtual Machines

Moving and Sharing Virtual Machines

The following sections provide information on how to move your virtual machines from one host to another or elsewhere on the same host; plus recommendations on how to share virtual machines with other users:

- Moving a Virtual Machine on page 243
  - Virtual Machines Use Relative Paths on page 243
  - Preparing your Virtual Machine for the Move on page 244
  - Moving a Virtual Machine to a New Host Machine on page 245
- Moving an Older Virtual Machine on page 246
  - Preparing Your Virtual Machine for the Move on page 246
  - Preparing the New Host Machine on page 247
  - Considerations for Moving Disks in Undoable Mode on page 248
- Sharing Virtual Machines with Other Users on page 250

Moving a Virtual Machine

What do you do if you have created a virtual machine using GSX Server and you want to move it to a different computer? Or even somewhere else on your host? The process is not difficult, and in most cases you can even move your virtual machine from a Windows host to a Linux host — or vice versa. Here's how.

Note: These instructions assume that you are using a virtual disk — stored in a set of `.vmdk` files on your host computer.

It's always safest to make backup copies of all the files in your virtual machine's folder (directory) before you start a process like this.

Caution: VMware recommends you do not migrate a Red Hat Linux 7.3 or 7.2 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. For more information, see the Known Issues sections under Red Hat Linux 7.3 Installation Guidelines on page 301 and Red Hat Linux 7.1 and 7.2 Installation Guidelines on page 304.

Virtual Machines Use Relative Paths

In GSX Server 1, the path names for all files associated with a virtual machine were absolute, or fully qualified, meaning the complete route to the files on the host was stored. For example, the absolute path to a virtual disk file stored on a Windows Server 2003 host would be `C:\Documents and Settings\<user name>\My Documents\My Virtual Machines\<machine name>\<machine name>.vmdk`.

With GSX Server 2, path names to files are relative, meaning the path to each file is relative to the currently active folder (directory). For example, if you are in the virtual machine's directory, the relative path to the first virtual disk file would be `<machine name>.vmdk`.

Note: You can still use absolute paths if you wish.

If you intend to move a virtual machine created in a VMware product other than GSX Server 2 or VMware Workstation 3.1 and later, please see Moving an Older Virtual Machine on page 246.

Preparing your Virtual Machine for the Move

1. Shut down the guest operating system and power off the virtual machine. If the virtual machine is suspended, resume it before you shut down the guest operating system.

   If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read Considerations for Moving Disks in Undoable Mode on page 248.

   Note: If your disks are using nonpersistent mode, you must also move the redo-log (`.REDO`) file to the new host computer. By default, it is located in your host operating system's `temp` directory.

2. If you are moving the virtual machine to a new host and are using its UUID for management purposes, take note of the existing UUID. For more information, see step 1 under Setting the UUID for a Virtual Machine that Is Being Moved on page 159.

3. Do one of the following:

   - If you are moving the virtual machine to a new host and have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. Otherwise, you need to have a way of moving the virtual disk (`.vmdk`) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs if they are not too large.

     Once you know how you are going to move the virtual machine, go to Moving a Virtual Machine to a New Host Machine on page 245.

   - If you are moving this virtual machine to another directory on this host, then you are ready to make the move. Copy all the files in the virtual machine's original directory to the new location. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

     To avoid networking conflicts, change the virtual machine's MAC address. For more information, see Changing the MAC Address of a Virtual Machine on page 428.

     Launch a GSX Server console and connect to the virtual machine in its new location.

Moving a Virtual Machine to a New Host Machine

1. Make sure GSX Server is installed and working correctly on the new host computer.
2. Locate the virtual disk files you are moving and copy them into the new virtual machine directory. Be sure to copy all the files in the virtual machine's original directory. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

   If, for some reason, you are *not* moving a file, make sure you do not have any relative or absolute paths pointing to file. Use the Configuration Editor and check to see if your virtual machine is pointing to the correct location for files you do not move.

   Note: You should always keep your `.vmdk` files in one place. So if you move them, move all of them together.

   Also, check to see you do not have any absolute paths pointing to any files you *are* moving.

   To determine whether any files are using absolute or relative paths, use the Configuration Editor. Select each device. Also, look at the location of the redo-log file.

   Note: If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read Considerations for Moving Disks in Undoable Mode on page 248.
3. Launch a GSX Server console and connect to the virtual machine in its new location. If you are using the virtual machine's UUID for management purposes, change the UUID. For more information, see Setting the UUID for a Virtual Machine that Is Being Moved on page 159.
4. To avoid networking conflicts, change the virtual machine's MAC address. For more information, see Changing the MAC Address of a Virtual Machine on page 428.

Moving an Older Virtual Machine

If you have created a virtual machine using GSX Server 1 or another VMware product (not including VMware Workstation 3.1 and later), and you want to move it to a different computer or to another directory on your host, you need to perform the following tasks.

Note: These instructions assume that you are using a virtual disk — stored in a set of `.vmdk` files on your host computer.

It's always safest to make backup copies of all the files in your virtual machine's folder (directory) before you start a process like this.

Preparing Your Virtual Machine for the Move

1. Be sure you know whether the virtual disk is set up as an IDE disk or a SCSI disk. You can check this in the Configuration Editor (**Settings** > **Configuration Editor**).

   Also, note the size of the virtual disk you are moving. You need this information when you prepare the new host machine, as described in the next section.

2. Shut down the guest operating system. If the virtual machine is suspended, resume it, then shut down the guest operating system.

   Note: Do not move a suspended virtual machine from one host to another.

3. If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read Considerations for Moving Disks in Undoable Mode on page 248.

4. If you have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. Otherwise, you need to have a way of moving the virtual disk (`.vmdk`) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs if they are not too large.

   Note: If your disks are in undoable mode and you have not committed or discarded your changes, you must also move the redo-log (`.REDO`) file to the new host computer.

Preparing the New Host Machine

1. Make sure GSX Server is installed and working correctly on the new host computer.
2. Locate the virtual disk files you're moving and copy them into the new virtual machine directory.

   Note: If your virtual machine is using disks in undoable mode, commit or discard your changes before moving the disk. If you cannot or do not want to commit or discard the changes, see Considerations for Moving Disks in Undoable Mode on page 248.
3. Run the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux Hosts) and select the appropriate guest operating system for the virtual machine you're moving.

   Choose the existing virtual disk for your hard drive. Select the **Use existing virtual disk** option in the wizard.
4. Select all appropriate network, floppy and CD-ROM settings and finish creating the virtual machine.
5. Launch a GSX Server console and connect to the new virtual machine you just created. If you are using the virtual machine's UUID for management purposes, change the UUID. For more information, see Setting the UUID for a Virtual Machine that Is Being Moved on page 159.
6. To avoid networking conflicts, change the virtual machine's MAC address. For more information, see Changing the MAC Address of a Virtual Machine on page 428.

Considerations for Moving Disks in Undoable Mode

Once you commit or discard changes made to a disk in undoable mode, you can move your disk between Linux and Windows host operating systems. You can also move your disk to different locations on your computer and to other computers with the same host operating system.

However, if you cannot or do not want to commit or discard the changes made to your undoable disk, note the following:

- You can always move a disk in undoable mode between host operating systems of the same general type (for example, between two Microsoft Windows systems, or between two Linux systems). In general, you must place the disk and its redo log in a folder (directory) that has a path name identical to that of the current folder (directory).
- You may be able to move the disk in undoable mode between Windows and Linux host systems, and move the disk to a different folder (directory) on your current system, if there is no path name information in the virtual machine's configuration file. This is true for virtual machines created under GSX Server 2; however, virtual machines created with older versions of GSX Server or any other VMware product (except for Workstation 3.1 and later) contain full path names.

Follow these steps to check the configuration and see whether or not you can move your undoable disk without committing or discarding changes:

1. Start a GSX Server console.

   If you are moving a disk in undoable mode from one computer to another computer, start the console on the computer that currently has your disk.

2. Open the configuration file for the virtual machine that uses the undoable mode disk you wish to move.

   In the GSX Server console window, select **File** > **Open** and choose the configuration file of the virtual machine with the disk you want to move.

3. Start the Configuration Editor.

   Select **Settings** > **Configuration Editor**.

4. Examine the entry for your virtual disk to see whether it includes a full path to the first virtual disk file. For example, on a Windows host, you might see a **Disk File** listing like this:

```
My Documents\My Virtual Machines\Windows Me\Windows Me.vmdk
```

Entries for SCSI disks are similar.

If your **Disk File** information resembles that above, with a full path to the first disk file, then as long as you have not committed or discarded changes to the undoable disk, note the following:

- You can move the disk to another computer of the same type (Windows to Windows).
- You must place the virtual machine's other files (`.vmx` and `.REDO` on Windows, `.cfg` and `.REDO` on Linux) in the same relative location on the new computer. In other words, if the virtual machine's files reside in `My Documents\My Virtual Machines\Windows 2000\` on the original host computer, you must place them in that same location on the new host computer.
- You cannot move the disk to a computer of a different type (Windows to Linux or vice versa).
- You cannot move the disk to another folder (directory) on the current system.

If your Disk File information does not contain a path, it looks like this:

```
Windows 2000.vmdk
```

If your disk entry resembles the one above (just a filename with a `.vmdk` extension), you can move the disk and redo log anywhere you wish.

Sharing Virtual Machines with Other Users

If you intend to have other users access your virtual machines, you should consider the following points:

- On Windows hosts, the virtual machine files should be in a location on a system that is accessible to those users. When you create a virtual machine, by default all the files associated with it are placed in `C:\Documents and Settings\<username>\My Documents\My Virtual Machines` on a Windows Server 2003 or Windows 2000 host; on a Windows NT host, the files are placed in `C:\WINNT\Profiles\<username>\Personal\My Virtual Machines\`. (One exception to this is the redo log file for a virtual disk in nonpersistent mode, which is located in your system's temp folder.) Other users typically do not have access to folders under `<username>`. When you configure the virtual machine in the New Virtual Machine Wizard, you can specify a location for the virtual machine elsewhere on your system or on the network.
- On Linux hosts, permissions for the virtual machine files — especially the configuration file (`.cfg`) and virtual disks (`.vmdk`) — should be set for other users according to how you want them to use the virtual machine. For instance, if you want users to run a virtual machine but not be able to modify its configuration, do not make the configuration file writable.
- If your virtual machine uses disks in nonpersistent mode, you should consider changing the location of the redo-log file, since by default it is placed in your temp directory, to which other users may not have access (redo logs for disks in undoable mode are placed in the same directory as the virtual machine's configuration file). To change the location of the redo log, complete the following steps.

  A. With the virtual machine powered off, open the Configuration Editor. Choose **Settings** > **Configuration Editor**.

  B. Click the **Options** tab (Windows hosts) or **Misc** panel (Linux hosts).

  C. Click **Browse** and select a directory that is shared with other users.

  D. Click **OK** to save the change and close the Configuration Editor.

  Note: Virtual machines with disks in nonpersistent mode perform better when the redo log is located in the system's temp directory.

10

Installing Guest Operating Systems

Choosing and Installing Guest Operating Systems

The following sections describe which operating systems are supported and unsupported for use as guests under GSX Server and provide notes on installing specific guest operating systems:

- Supported and Unsupported Guest Operating Systems on page 254
  - Supported Guest Operating Systems on page 254
  - Unsupported Guest Operating Systems on page 255
- Installation Notes for Particular Guest Operating Systems on page 256
  - Windows Server 2003 Installation Guidelines on page 257
  - Windows XP Installation Guidelines on page 260
  - Windows 2000 Installation Guidelines on page 263
  - Windows NT Installation Guidelines on page 266
  - Windows Me Installation Guidelines on page 270
  - Windows 98 Installation Guidelines on page 272
  - Windows 95 Installation Guidelines on page 275
  - DOS and Windows 3.1x Installation Notes on page 280
  - Mandrake Linux 9.1 Installation Guidelines on page 282
  - Mandrake Linux 9.0 Installation Guidelines on page 284
  - Mandrake Linux 8.2 Installation Guidelines on page 286
  - Mandrake Linux 8.0 and 8.1 Installation Guidelines on page 288
  - Red Hat Enterprise Linux 2.1 Installation Guidelines on page 291
  - Red Hat Linux 9.0 Installation Guidelines on page 294
  - Red Hat Linux 8.0 Installation Guidelines on page 298
  - Red Hat Linux 7.3 Installation Guidelines on page 301
  - Red Hat Linux 7.1 and 7.2 Installation Guidelines on page 304
  - Red Hat Linux 7.0 Installation Guidelines on page 307
  - Red Hat Linux 6.x Installation Guidelines on page 310
  - SuSE Linux Enterprise Server 8 Installation Guidelines on page 312

- SuSE Linux 8.2 Installation Guidelines on page 314
- SuSE Linux 8.1 Installation Guidelines on page 316
- SuSE Linux 8.0 Installation Guidelines on page 319
- SuSE Linux Enterprise Server 7 Installation Guidelines on page 322
- SuSE Linux 7.3 Installation Guidelines on page 324
- SuSE Linux 7.2 Installation Guidelines on page 326
- SuSE Linux 7.1 Installation Guidelines on page 328
- SuSE Linux 7.0 Installation Guidelines on page 330
- SuSE Linux 6.3 and 6.4 Installation Guidelines on page 332
- SuSE Linux 6.2 Installation Guidelines on page 334
- SuSE Linux 6.1 Installation Guidelines on page 336
- SuSE Linux 6.0 Installation Guidelines on page 338
- Turbolinux 7.0 Installation Guidelines on page 339
- Turbolinux 6.0 Installation Guidelines on page 341
- NetWare 6.0 and 6.5 Server Installation Guidelines on page 343
- NetWare 5.1 Server Installation Guidelines on page 347
- NetWare 4.2 Server Installation Guidelines on page 351
- FreeBSD Installation Guidelines on page 355

Supported and Unsupported Guest Operating Systems

Check the lists that follow for information on which operating systems now work as guest operating systems in a GSX Server virtual machine and the status of operating systems that are not on the supported list.

Supported Guest Operating Systems

Microsoft Windows Server 2003

- Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Editionand Windows Server 2003 Web Edition

Microsoft Windows XP

- Windows XP Home and Windows XP Professional Edition, including Service Pack 1

Microsoft Windows 2000

- Windows 2000 Professional, Windows 2000 Server and Windows 2000 Advanced Server; Service Pack 2, Service Pack 3 and Service Pack 4

Microsoft Windows NT

- Windows NT 4.0 Workstation and Windows NT Server, Service Pack 3 or higher

Microsoft Windows

- Windows Millennium Edition
- Windows 98 and Windows 98 SE
- Windows 95 (all OSR releases)
- Windows for Workgroups
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6

Linux

- Mandrake Linux 8.0, 8.1, 8.2, 9.0 and 9.1
- Red Hat Linux 6.2, 7.0, 7.1, 7.2, 7.3, 8.0, 9.0 and Red Hat Enterprise Linux (AS, ES, WS) 2.1
- SuSE Linux 6.0, 6.1, 6.2, 6.3, 6.4, 7.0, 7.1, 7.2, 7.3, 8.0, 8.1, 8.2 and SLES 7, 8

- Turbolinux 6.0 and 7.0

FreeBSD

- FreeBSD 3.1, 4.0, 4.1, 4.2, 4.3, 4.4 and 4.5

NetWare

- NetWare 4.2, 5.1, 6.0 and 6.5

Unsupported Guest Operating Systems

Note: GSX Server provides support only for guest operating systems that run on x86 (Intel and compatible) microprocessors. It is not possible to use an operating system designed for a different type of microprocessor as a guest operating system. For example, Mac OS, designed to run on PowerPC processors, is not supported. Similarly, operating systems designed to run on the Alpha microprocessor are not supported.

Operating Systems that May Work but are Not Supported

The following guest operating systems may work with GSX Server but are not supported.

- Caldera OpenLinux 1.3
- Novell NetWare 5.0 (on a Pentium III processor, only works with a Novell-supplied patch; for more information, see *support.novell.com/cgi-bin/search/searchtid.cgi?/2958591.htm*)
- Solaris 7 Intel Edition, 8
- NetBSD 1.x
- OpenBSD 2.x
- Turbolinux 8.0

Operating Systems that May Not Work and for which Support is Not Planned

The following guest operating systems may not work with GSX Server. There are currently no plans to support these guests in the near future.

- BeOS
- IBM OS/2 and OS/2 Warp
- Minix
- QNX
- SCO Unix
- UnixWare

Installation Notes for Particular Guest Operating Systems

Installing a guest operating system inside your GSX Server virtual machine is essentially the same as installing it on a physical computer.

One suggestion VMware recommends you take before you start installing the guest operating system is to disable the screen saver on the host.

The basic steps for a typical operating system are:

1. Run GSX Server in a local console.
2. Create a new virtual machine.
3. Insert the installation CD-ROM or floppy disk for your guest operating system into the appropriate drive on your GSX Server host.
4. Power on your virtual machine by clicking the **Power On** button.
5. Follow the instructions provided by the operating system vendor.

As with physical computers, a separate operating system license is required for each virtual machine you run.

This section provides notes that highlight special steps you may need to take when you install particular guest operating systems.

Windows Server 2003 Installation Guidelines

You can install Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition and Windows Server 2003 Web Edition in a virtual machine using the corresponding Windows Server 2003 distribution CD.

Note: Some Microsoft Windows Server 2003 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows Server 2003 operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

Note: To use SCSI disks in a Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows Server 2003. If you have a virtual machine with a SCSI virtual disk and a Windows 9x, Windows Me, Windows NT or Windows 2000 guest operating system and want to upgrade it to Windows Server 2003, install the new SCSI driver before upgrading the operating system.

Installation Steps

If you want to run Windows Server 2003 in a GSX Server virtual machine, be sure you have a full installation CD for the operating system.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installing the Guest Operating System

1. Before starting the installation, use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect. For example, if you would like networking software to be installed during the Windows Server 2003 installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows Server 2003 installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine to start installing Windows Server 2003.
4. Follow the installation steps as you would for a physical machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Enabling Sound in a Windows Server 2003 Guest

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

In addition, Windows Server 2003 does not automatically detect and install drivers for ISA sound cards, such as the Creative Labs Sound Blaster emulated in a virtual machine. For details on installing the driver for the virtual machine's sound card, see Sound in a Windows XP or Windows Server 2003 Guest on page 476.

Enabling Networking After Installing Windows Server 2003

If networking was disabled at the time you installed your Windows Server 2003 guest operating system, you can enable it after the operating system has been installed. For more information, see Adding and Modifying Virtual Network Adapters on page 415.

Choosing the Network Driver for Your Virtual Machine

Two networking drivers are available for Windows Server 2003 guest operating systems: the `vlance` driver, that is available for all virtual machines and is installed automatically, and the `vmxnet` driver, which is available only for Windows Server 2003, Windows XP and Windows 2000 virtual machines. The `vmxnet` driver provides better networking performance. The difference in networking performance is most noticeable if the virtual machine is connected to a Gigabit Ethernet card.

To install the `vmxnet` driver, see Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems on page 441.

Known Issues

- The Microsoft Windows Server 2003 product activation feature creates a numerical key based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine may require you to reactivate the operating system. There are some steps you can take to minimize the number of significant changes.
  - Set the final memory size for your virtual machine before you activate Windows Server 2003. When you cross certain thresholds — approximately 32MB, 64MB, 128MB, 256MB, 512MB and 1GB — the product activation feature sees the changes as significant.

Note: The size reported to the Windows product activation feature is slightly less than the actual amount configured for the virtual machine. For example, 128MB is interpreted as falling in the 64MB–127MB range.

- Install VMware Tools before you activate Windows Server 2003. When the SVGA driver in the VMware Tools package is installed, it activates features in the virtual graphics adapter that make it appear to Windows Server 2003 as a new graphics adapter.
- If you want to experiment with any other aspects of the virtual machine configuration — for example, you want to add more virtual disks — do so before activating Windows Server 2003. Keep in mind that you have 30 days for experimentation before you have to activate the operating system.

For more details on Windows Server 2003 product activation, see the Microsoft Web site.

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- The hibernation feature is not supported in this release of GSX Server. Instead of using the guest operating system's hibernate feature, suspend the virtual machine by clicking **Suspend** on the console toolbar.
- In order to install and run a checked (debug) build of Windows Server 2003 in a virtual machine, you must first edit the virtual machine's configuration file (`.vmx` on Windows hosts, `.cfg` on Linux hosts). Add the following line:
  `uhci.forceHaltBit = TRUE`
- Windows Server 2003 disables hardware acceleration by default. This slows down graphics performance and mouse responsiveness in the guest operating system.

  To enable hardware acceleration in a Windows Server 2003 guest, open the Control Panel, then open the Display Properties control panel. On the **Settings** tab, click **Advanced**. On the **Troubleshoot** tab, drag the **Hardware acceleration** slider all the way to **Full**.

Windows XP Installation Guidelines

You can install Windows XP Home Edition or Professional in a virtual machine using the corresponding Windows XP distribution CD.

Note: Some Microsoft Windows XP OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows XP operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows XP to install in your virtual machine.

Note: To use SCSI disks in a Windows XP virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP. If you have a virtual machine with a SCSI virtual disk and a Windows 9x, Windows Me, Windows NT or Windows 2000 guest operating system and want to upgrade it to Windows XP, install the new SCSI driver before upgrading the operating system.

Installation Steps

If you want to run Windows XP Home Edition or Professional in a GSX Server virtual machine, be sure you have a full installation CD for the operating system.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts). Make sure you selected Windows XP as your guest operating system.

Now you're ready to install Windows XP Home Edition or Professional.

Installing the Guest Operating System

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Windows XP installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine to start installing the guest operating system.
4. Follow the installation steps as you would for a physical machine, except as noted in the following steps.

5. After the system reboots, a message balloon asks if you want Windows to automatically correct your screen resolution and color depth setting. Do not make the change at this time. You cannot change resolution and color depth until you have installed the VMware SVGA driver — part of the VMware Tools package.
6. Run the VMware Tools installer. For details, see Installing VMware Tools on page 113.
7. When the guest operating system reboots, allow it to change the screen resolution and color depth setting.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details on installing VMware Tools, see Installing VMware Tools on page 113.

Enabling Sound in a Windows XP Guest

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

In addition, Windows XP does not automatically detect and install drivers for ISA sound cards, such as the Creative Labs Sound Blaster emulated in a virtual machine. For details on installing the driver for the virtual machine's sound card, see Sound in a Windows XP or Windows Server 2003 Guest on page 476.

Enabling Networking After Installing Windows XP

If networking was disabled at the time you installed your Windows XP guest operating system, you can enable it after the operating system has been installed. For more information, see Adding and Modifying Virtual Network Adapters on page 415.

Choosing the Network Driver for Your Virtual Machine

Two networking drivers are available for Windows XP guest operating systems: the `vlance` driver, that is available for all virtual machines and is installed automatically, and the `vmxnet` driver, which is available only for Windows Server 2003, Windows XP and Windows 2000 virtual machines. The `vmxnet` driver provides better networking performance. The difference in networking performance is most noticeable if the virtual machine is connected to a Gigabit Ethernet card.

To install the `vmxnet` driver, see Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems on page 441.

Known Issues

- The Microsoft Windows XP product activation feature creates a numerical key based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine may require you to reactivate the operating system. There are some steps you can take to minimize the number of significant changes.
  - Set the final memory size for your virtual machine before you activate Windows XP. When you cross certain thresholds — approximately 32MB, 64MB, 128MB, 256MB, 512MB and 1GB — the product activation feature sees the changes as significant.

    Note: The size reported to the Windows product activation feature is slightly less than the actual amount configured for the virtual machine. For example, 128MB is interpreted as falling in the 64MB–127MB range.
  - Install VMware Tools before you activate Windows XP. When the SVGA driver in the VMware Tools package is installed, it activates features in the virtual graphics adapter that make it appear to Windows XP as a new graphics adapter.
  - If you want to experiment with any other aspects of the virtual machine configuration — for example, you want to add more virtual disks — do so before activating Windows XP. Keep in mind that you have 30 days for experimentation before you have to activate the operating system.

  For more details on Windows XP product activation, see the Microsoft Web site.
- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- The hibernation feature is not supported in this release. Instead of using the guest operating system's hibernate feature, suspend the virtual machine by clicking **Suspend** on the console toolbar.
- In order to install and run a checked (debug) build of Windows XP in a virtual machine, you must first edit the virtual machine's configuration file (`.vmx` on Windows hosts, `.cfg` on Linux hosts). Add the following line:
  `uhci.forceHaltBit = TRUE`

Windows 2000 Installation Guidelines

You can install Windows 2000 Professional, Server or Advanced Server in a virtual machine using the corresponding Windows 2000 distribution CD.

Note: Some Microsoft Windows 2000 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 2000 operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Windows 2000 Installation Steps

1. Before starting the installation, use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect. For example, if you would like networking software to be installed during the Windows 2000 installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 2000 installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine to start installing Windows 2000.
4. If you enabled the virtual machine's Ethernet adapter, an AMD PCNET Family Ethernet Adapter is detected and set up automatically.

VMware Tools

Be sure to install VMware Tools in your guest operating system. After you install VMware Tools, you need to change your Windows 2000 screen area to be greater than 640x480 pixels; if you do not change it, Windows 2000 uses the standard VGA driver, and your performance will suffer.

For details, see Installing VMware Tools on page 113.

Enabling Sound After Installing Windows 2000

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Enabling Networking After Installing Windows 2000

If networking was disabled at the time you installed your Windows 2000 guest operating system, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows 2000 and power off the virtual machine.
2. From the GSX Server console window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. When Windows 2000 boots, it automatically detects a new network adapter and loads drivers for an AMD PCNET Family PCI Ethernet Adapter.
6. You should be able to access the network after logging on to the Windows 2000 guest operating system.

Linux Host

1. Shut down Windows 2000 and power off the virtual machine.
2. From the GSX Server console window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click **Install**.
4. Click **OK** to save the updated configuration.
5. Power on the virtual machine.
6. When Windows 2000 boots, it automatically detects a new network adapter and loads drivers for an AMD PCNET Family PCI Ethernet Adapter.
7. You should be able to access the network after logging on to the Windows 2000 guest operating system.

Choosing the Network Driver for Your Virtual Machine

Two networking drivers are available for Windows 2000 guest operating systems: the `vlance` driver, that is available for all virtual machines and is installed automatically, and the `vmxnet` driver, which is available only for Windows Server 2003, Windows XP and Windows 2000 virtual machines. The `vmxnet` driver provides better networking performance. The difference in networking performance is most noticeable if the virtual machine is connected to a Gigabit Ethernet card.

To install the `vmxnet` driver, see Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems on page 441.

Known Issues

- If the installation of the guest operating system hangs, search our Knowledge Base at *www.vmware.com/support/kb/enduser/std_alp.php* for a possible answer to your problem.
- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Windows NT Installation Guidelines

You can install Windows NT 4.0 (Workstation or Server) in a virtual machine using the standard Windows NT CD.

Note: Some Microsoft Windows NT OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows NT operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows NT to install in your virtual machine.

Note: If you are going to run a Windows NT virtual machine with IDE virtual disks on a multiprocessor host computer, you may notice slower than expected disk input/output performance. For more information, see Disk Performance in Windows NT Guests on Multiprocessor Hosts on page 402.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Windows NT Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Windows NT installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows NT installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine to start installing Windows NT.
4. If you have enabled the virtual machine's Ethernet Adapter, an AMD PCNET Family Ethernet Adapter is detected and set up automatically. The default settings should work fine and do not need to be changed.
5. Finish the Windows NT installation.
6. GSX Server's virtual disks support DMA transfers for better performance.

   You can enable the feature after Windows NT has been successfully installed. You need the NT Service Pack 3 or 4 CD to enable this option. Once the virtual machine is running Windows NT, insert the SP3 or SP4 CD in the drive, run `DMACHECK.EXE` from the `\SUPPORT\UTILS\I386` folder on the CD and

click the **Enabled** option for the IDE controller/channel that is configured with the virtual disk (typically channel 0 only, unless you have the virtual machine configured with multiple virtual disks). The DMA option should not be enabled for any IDE channel that has a CD-ROM drive configured for it. Enabling it causes an error.

Note: DMA is always enabled on SCSI virtual disks.

Note: If you have a virtual disk and a CD-ROM attached as master and slave to the primary IDE controller (channel 0) and you want to enable DMA, power off the virtual machine and use the Configuration Editor to move the CD-ROM to the secondary IDE controller (channel 1) at IDE 1:0. Then boot the virtual machine with Windows NT, run `DMACHECK` and enable DMA for channel 0 only.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Setting Up a Windows NT 4.0 Guest with Multiple Disks

To set up a virtual machine running Windows NT 4.0 and using multiple disks, you must first create a virtual machine with only one disk. Install Windows NT on that disk. Then use the Configuration Editor (**Settings** > **Configuration Editor**) to add the additional disks.

In addition, note that if you have a Windows NT 4.0 guest with a SCSI virtual disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

Enabling Sound After Installing Windows NT

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Enabling Networking After Installing Windows NT

If networking was disabled at the time you installed Windows NT, you can enable it after the operating system has been installed. For more information, see Adding and Modifying Virtual Network Adapters on page 415.

Windows Host

1. Shut down Windows NT and power off the virtual machine.
2. From the GSX Server console window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.

3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. While Windows NT is booting, insert the Windows NT 4.0 installation CD in the CD-ROM drive.
6. Log on to Windows NT and install the AMD PCNET driver:
   A. Open the Network properties page by double-clicking the Network icon in Control Panel. Change to the Network Adapters screen by clicking the **Adapters** tab.
   B. Click the **Add** button and select the AMD PCNET Family Ethernet Adapter from the list.
   C. A message pops up prompting you to enter a path for the Windows NT files. Specify the `\I386` folder on the CD in the path you enter (for example, type `D:\i386` if the CD is in drive D) and click **Continue**.
   D. Windows NT setup prompts you for the Windows NT files again. Click **Continue**.
   E. Use the default adapter settings; they do not need to be changed. Windows NT setup prompts you again for a path to the Windows NT files. Click **Continue** to finish installing the driver.

Linux Host

1. Shut down Windows NT and power off the virtual machine.
2. From the console window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click **Install**.
4. Click **OK** to save the updated configuration.
5. Power on the virtual machine.
6. While Windows NT is booting, insert the Windows NT 4.0 installation CD in the CD-ROM drive.
7. Log on to Windows NT and install the AMD PCNET driver:
   A. Open the Network properties page by double-clicking the Network icon in Control Panel. Change to the Network Adapters screen by clicking the **Adapters** tab.

B. Click the **Add** button and select the AMD PCNET Family Ethernet Adapter from the list.

C. A message pops up prompting you to enter a path for the Windows NT files. Specify the `\I386` folder on the CD in the path you enter (for example, type `D:\i386` if the CD is in drive D) and click **Continue**.

D. Windows NT setup prompts you for the Windows NT files again. Click **Continue**.

E. Use the default adapter settings; they do not need to be changed. Windows NT setup prompts you again for a path to the Windows NT files. Click **Continue** to finish installing the driver.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Windows Me Installation Guidelines

You can install Windows Millennium Edition in a virtual machine using the standard Windows Me CD.

Note: Some Microsoft Windows Me OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows Me operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows Me to install in your virtual machine.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows Me Setup program to install networking services, be sure that a virtual Ethernet adapter is installed in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows Me installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine to start installing Windows Me.
4. Choose to boot from CD-ROM, then select the **Start Windows Me Setup from CD-ROM** option. The setup program runs `FDISK` and reboots.
5. Once again, choose to boot from CD-ROM, then select the **Start Windows Me Setup from CD-ROM** option. The setup program continues installing Windows Me.
6. Follow the Windows Me installation steps as you would for a physical machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Enabling Sound After Installing Windows Me

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has

been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Enabling Networking After Installing Windows Me

If networking was disabled at the time you installed your Windows Me guest operating system, you can enable it after the operating system has been installed. For more information, see Adding and Modifying Virtual Network Adapters on page 415.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Windows 98 Installation Guidelines

You can install Windows 98 in a virtual machine using the standard Windows 98 CD.

Note: Some Microsoft Windows 98 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 98 operating system on your actual computer, you may not be able to install it in a GSX Server virtual machine. You may need to purchase a new copy of Windows 98 to install in your virtual machine.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows 98 setup program to install a sound driver, be sure that sound is enabled in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 98 installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine to start installing Windows 98.
4. Choose to boot from CD-ROM, then select the **Start Windows 98 Setup from CD-ROM** option. The setup program runs `FDISK` and reboots.
5. Once again, choose to boot from CD-ROM, then select the **Start Windows 98 Setup from CD-ROM** option. The setup program continues installing Windows 98.
6. Follow the Windows 98 installation steps as you would for a physical PC.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Enabling Sound After Installing Windows 98

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Enabling Networking After Installing Windows 98

If networking was disabled at the time you installed Windows 98, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows 98 and power off the virtual machine.
2. From the GSX Server console window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. When Windows 98 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI-ISA) and prompts for the Windows 98 CD-ROM to install drivers. The default Ethernet adapter settings should work fine and do not need to be changed.
6. Use the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 98 does not install it by default.

Linux Host

1. Shut down Windows 98 and power off the virtual machine.
2. From the console window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click **Install**.
4. Click **OK** to save the updated configuration.
5. Power on the virtual machine.
6. When Windows 98 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI-ISA) and prompts for the Windows 98 CD-ROM to install drivers. The default Ethernet adapter settings should work fine and do not need to be changed.
7. Use the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 98 does not install it by default.

Known Issues

- After Windows 98 has been installed, you may notice COM5 and COM6 devices exist within the Windows Device Manager. These devices do not actually exist and are not consuming IRQ or other resources. You may remove them using the Windows device manager if you like.
- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- Support for `EMM386.EXE` and other memory managers is currently limited. If you initially boot using a customized non-standard MS-DOS or Windows 98 boot floppy, be sure that `EMM386.EXE` (or other memory manager) is not being loaded. `HIMEM.SYS` and `RAMDRIVE.SYS` can be loaded and used without problems.

Windows 95 Installation Guidelines

You can install Windows 95 in a virtual machine using a standard Windows 95 boot floppy and CD-ROM.

Note: Some Microsoft Windows 95 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 95 operating system on your actual computer, you may not be able to install it within a GSX Server virtual machine. You may need to purchase a new copy of Windows to install within a virtual machine.

Note: Some Windows 95 distributions provide instructions that do not include the steps to `FDISK` and `FORMAT` a `C:` drive. You must `FDISK` and `FORMAT` the GSX Server virtual hard disk drives before running Windows 95 setup.

The instructions below are for the simplest case of one virtual IDE hard drive and one virtual IDE CD-ROM drive. If you have configured the virtual machine with more than one IDE hard drive, you should also `FDISK` and `FORMAT` these drives before installing Windows 95. If you have configured the virtual machine with more than one virtual hard drive or more than one virtual CD-ROM, you may need to use different device letters than those in the instructions below.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows 95 setup program to install a sound driver, be sure that sound is enabled in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 95 CD-ROM Setup Boot Disk in floppy drive `A:` and insert the Windows 95 installation CD in the CD-ROM drive on your GSX Server host.
3. Power on the virtual machine.
4. After the virtual machine boots, if you are presented with a choice of CD-ROM drivers, select the first IDE driver option available (even if your computer has a SCSI CD-ROM drive).

5. Partition the virtual disk.
   `A:\> FDISK`
   Answer the questions.

   Note: If you create a primary partition that is smaller than the size of the hard disk, be sure the partition is marked active.

6. Reboot Windows 95. If the cursor is not already within the GSX Server console window, click in the window, then press Ctrl-Alt-Ins on a Windows host or Ctrl-Alt-Del on a Linux host. If prompted on reboot to select a CD-ROM driver, select the first IDE CD-ROM driver from the list.

7. Format the `C:` drive.
   `A:\> FORMAT C: /S`

8. Start the Windows 95 installation.
   `A:\> D:\WIN95\SETUP /IS`

   Note: An intermittent problem can occur during Windows 95 installations in a virtual machine. Shortly after the Windows 95 Setup program is started, Scandisk runs to completion, and when the Windows 95 Setup program should start its graphical user interface, the virtual machine returns to an MS-DOS prompt. VMware recommends you reboot the virtual machine and rerun Windows 95 Setup. You do not need to `FDISK` or `FORMAT` the drive again. If this problem occurs reproducibly, please report it to VMware technical support.

9. If the virtual machine's Ethernet adapter is enabled, you have to manually add an Ethernet driver because Windows 95 does not detect it during the Analyzing Computer phase (even if you selected the Network Adapter detection option). Do the following to enable networking:

   A. Continue with the Windows 95 installation, until you get to the Windows 95 Setup Wizard/Setup Options screen. Change the default setting from **Typical** to **Custom** and click **Next** to continue.

   B. From the Network Configuration screen (which appears after the Analyzing Computer phase), click **Add**, select the **Adapter** component, select **Advanced Micro Devices** from the manufacturer window and **AMD PCNET Family Ethernet Adapter(PCI&ISA)** from the network adapter window.

   C. If you need TCP/IP networking, add it from the Network Configuration screen (Windows 95 Setup does not enable TCP/IP by default). If you don't do this, the first phase of the Windows 95 installation does not copy some of the files it will need later, and the entire installation fails.

Also be sure that the Microsoft NetBEUI protocol is installed. It may not be installed by default.

10. Finish the Windows 95 installation.
11. GSX Server's virtual disks support DMA transfers for better performance. The feature can be enabled after Windows 95 has been successfully installed on a virtual IDE disk. Follow these steps to enable the feature:
    A. Right-click My Computer and select **Properties**.
    B. From the System Properties dialog box, click the **Device Manager** tab.
    C. Double-click the **Disk Drives** device category.
    D. Double-click the **GENERIC IDE DISK TYPE01** device.
    E. Click the **Settings** tab and select the **DMA** check box.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Enabling Sound After Installing Windows 95

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Enabling Networking After Installing Windows 95

If networking was disabled at the time you installed Windows 95, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows 95 and power off the virtual machine.
2. From the GSX Server console window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. When Windows 95 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI&ISA) and prompts for the Windows 95 CD-ROM to install drivers.

The default Ethernet adapter settings should work fine and do not need to be changed.

6. Double-click the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 95 does not install it by default.

Linux Host

1. Shut down Windows 95 and power off the virtual machine.
2. From the console window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click **Install**.
4. Click **OK** to save the updated configuration.
5. Power on the virtual machine.
6. When Windows 95 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI&ISA) and prompts for the Windows 95 CD-ROM to install drivers. The default Ethernet adapter settings should work fine and do not need to be changed.
7. Double-click the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 95 does not install it by default.

Known Issues

- After Windows 95 has been installed, you may find that networking is not working in the guest operating system. There are several things you should check.
  - Either remove your virtual machine's virtual USB adapter using the Configuration Editor (**Settings** > **Configuration Editor**) or — if your release of Windows 95 includes USB support — be sure the USB drivers are installed.
  - Check the Windows 95 Device Manager to see if COM5 and COM6 devices are listed. If they are, disable or remove them.
  - Be sure that NetBEUI was installed when you set up networking.
  - Be sure that Windows 95 Plug and Play properly detected the virtual Ethernet adapter. If it did not, you may need to use the Device Manager to remove the adapter, then reinstall it using the Add New Hardware control panel.

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- After Windows 95 has been installed, you may notice Unknown devices exist in the Windows Device Manager. These devices do not actually exist and are not consuming IRQ or other resources. You may remove them using the Windows Device Manager if you like.
- Support for EMM386.EXE and other memory managers is currently limited. If you plan to boot initially using a customized non-standard MS-DOS or Windows 95 boot disk, be sure that `EMM386.EXE` (or other memory manager) is not being loaded. `HIMEM.SYS` and `RAMDRIVE.SYS` can be loaded and used without problems.

DOS and Windows 3.1x Installation Notes

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

DOS Installation Notes

You can install MS-DOS 6.22 inside a virtual machine using the MS-DOS installation disks provided with the full version. If you have the upgrade disks, you must install an earlier version of DOS before you upgrade. To start installing MS-DOS 6.22, put the first disk in the floppy drive, power on the virtual machine and follow the instructions on the screen.

After you install DOS, VMware recommends that you install a CPU idle program within the virtual machine. Most versions of DOS do not idle the CPU when they are idle. Therefore, when you are running DOS in a virtual machine, the virtual machine takes up CPU time on the host even when DOS is idle. GSX Server relies on the guest operating system to use the Halt instruction or advanced power management to deschedule the virtual machine when it is idle.

We have tested a program called `DOSIDLE.EXE` and have found it works successfully with GSX Server. It can be downloaded from *www.vmware.com/software/dosidle210.zip*.

Follow the instructions provided with the `DOSIDLE.EXE` program. But be aware of the `-cpu` option, which causes the idle program to access the CPU at a low level in order to optimize performance. There is a good chance that this will not work with some CPUs under GSX Server. VMware suggests that you not use it.

Windows 3.1x Installation Notes

You can install Windows 3.1x using the standard installation disks. GSX Server virtual machines support the networking features found in Windows 3.11 (or Windows for Workgroups). If you set up networking, choose the Advanced Micro Devices PCNET Family (NDIS2/NDIS3) Ethernet driver.

Enabling Sound After Installing the Guest Operating System

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

- The current support for `DOS/EMM386` is limited. We recommend that you avoid using it. Be sure to comment out the entry in the `CONFIG.SYS` file.
- You may intermittently encounter erratic mouse behavior in virtual machines running Windows 3.1x in window mode. This problem does not appear in full screen mode in a local console.
- No VMware Tools package exists for DOS or Windows 3.1x guest operating systems; therefore, Windows 3.1x is limited to VGA mode graphics and you must always use the Ctrl-Alt key combination to release the mouse from a DOS or Windows 3.1x virtual machine.
- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Mandrake Linux 9.1 Installation Guidelines

The easiest method of installing Mandrake Linux 9.1 in a virtual machine is to use the standard Mandrake Linux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Mandrake Linux 9.1 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Mandrake Linux 9.1 installation, you are offered a choice of XFree86 X servers. You may choose either one, but do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Mandrake Linux 9.1.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Mandrake Linux 9.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. You may also want to increase the virtual machine's memory to 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Mandrake Linux 9.1 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In the partitioning step, unless you have special requirements, it is all right to let Mandrake Linux auto-allocate the space. Select **Use free space**.
5. When you reach the Summary screen, configure the graphical interface and the boot loader.
6. On the Graphical Interface line, click **Configure** to launch a wizard. In the wizard, make the following selections:
   - The resolution and refresh rate you want your guest to use
   - VMware virtual video card
   - XFree 4.3
   - **No** when asked if you want to test the configuration

- **No** when asked if you want to start X when you reboot

7. On the Bootloader line, click **Configure**. When selecting a boot loader, use **LILO with text menu**. Do not use the graphical version of LILO. It causes the virtual machine to hang.
8. When the installer asks if you want to install updates to the packages, answer **No**.

This completes basic installation of the Mandrake Linux 9.1 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Note: With a Mandrake Linux 9.1 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

Note: Provided you installed the XFree 4.3 X server when you installed the guest operating system (as advised in the install steps), when you start the VMware Tools installation script (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Mandrake Linux 9.0 Installation Guidelines

The easiest method of installing Mandrake Linux 9.0 in a virtual machine is to use the standard Mandrake Linux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Mandrake Linux 9.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Mandrake Linux 9.0 installation, you are offered a choice of XFree86 X servers. You may choose either one, but do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Mandrake Linux 9.0.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Mandrake Linux 9.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. You may also want to increase the virtual machine's memory to 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Mandrake Linux 9.0 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Use the Expert installer.
5. In the partitioning step, unless you have special requirements, it is all right to let Mandrake Linux auto-allocate the space.
6. When selecting a boot loader, use **LILO with text menu**. Do not use the graphical version of LILO. It causes the virtual machine to hang.
7. Do not create a custom boot disk when prompted.
8. You are offered a choice of 2 XFree86 X servers to install. Choose **XFree 4.2.0**. This driver recognizes the VMware SVGA driver.
9. Near the end of the installation, after files have been copied, you reach the monitor setup screen. Choose the resolution and refresh rate you want your guest to use.

10. When the installer asks if you want to test the configuration, answer **No**.
11. When the installer asks whether to start X when you reboot, answer **No**.
12. When the installer asks if you want to install updates to the packages, answer **No**.

This completes basic installation of the Mandrake Linux 9.0 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Note: With a Mandrake Linux 9.0 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

Note: Provided you installed the XFree 4.2.0 X server when you installed the guest operating system (as advised in the install steps), when you start the VMware Tools installation script (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Mandrake Linux 8.2 Installation Guidelines

The easiest method of installing Mandrake Linux 8.2 in a virtual machine is to use the standard Mandrake Linux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Mandrake Linux 8.2 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Mandrake Linux 8.2 installation, you are offered a choice of XFree86 X servers. Choose XFree 4.2.0, but do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Mandrake Linux 8.2.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Mandrake Linux 8.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. You may also want to increase the virtual machine's memory to 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Mandrake Linux 8.2 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Use the Expert installer.
5. In the partitioning step, unless you have special requirements, it is all right to let Mandrake Linux auto-allocate the space.
6. When selecting a boot loader, use **LILO with text menu**. Do not use the graphical version of LILO. It causes the virtual machine to hang.
7. Do not create a custom boot disk when prompted.
8. You are offered a choice of 2 XFree86 X servers to install. Choose **XFree 4.2.0**. This driver recognizes the VMware SVGA driver.
9. Near the end of the installation, after files have been copied, you reach the monitor setup screen. Choose the resolution and refresh rate you want your guest to use.

10. When the installer asks if you want to test the configuration, answer **No**.
11. When the installer asks if you want to install updates to the kernel, answer **No**.
12. When the installer asks whether to start X when you reboot, answer **No**.

This completes basic installation of the Mandrake Linux 8.2 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Note: With a Mandrake Linux 8.2 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

Note: Provided you installed the XFree 4.2.0 X server when you installed the guest operating system (as advised in the install steps), when you start the VMware Tools installation program (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Enabling Sound After Installing Mandrake Linux 8.2

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Mandrake Linux 8.0 and 8.1 Installation Guidelines

The easiest method of installing Mandrake Linux 8.0 or 8.1 in a virtual machine is to use the standard Mandrake Linux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Mandrake Linux 8.0 or 8.1 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Mandrake Linux 8.0 or 8.1 installation, you are offered a choice of XFree86 X servers. You may choose either one, but do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Mandrake Linux 8.0 or 8.1 and create one symbolic link as described in the steps that follow.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Mandrake Linux 8.0 or 8.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. You may also want to increase the virtual machine's memory to 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Mandrake Linux 8.0 or 8.1 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Use the Expert installer.
5. In the partitioning step, unless you have special requirements, it is all right to let Mandrake Linux auto-allocate the space.
6. When selecting a boot loader, use **LILO with text menu**. Do not use the graphical version of LILO. It causes the virtual machine to hang.
7. On the Select a Graphic Card screen, choose **Other > Generic VGA compatible**.
8. Near the end of the installation, after files have been copied, you reach the monitor setup screen. Choose **Super VGA, 800x600 @ 56 Hz**.
9. When the installer asks whether to start X when you reboot, answer **No**.

This completes basic installation of the Mandrake Linux 8.0 or 8.1 guest operating system. But there are two additional steps that are vital if you want to run X in your virtual machine.

10. Install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

    Note: With a Mandrake Linux 8.0 or 8.1 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools and carried out the final step in this guide.

11. Be sure you are logged on as root (`su`), then take the following steps to set up a symbolic link to the correct XFree86 configuration file.

    ```
    cd /etc
    ln -s /etc/X11/XF86Config.vm XF86Config
    ```

    Use the `startx` command to start your X server.

Enabling Sound After Installing Mandrake Linux 8.0 or 8.1

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- The shutdown process in the guest operating system may hang when shutting down the network interface because of the way the Mandrake Linux 8.0 shutdown script handles `dhcpd`. This problem does not occur with Mandrake Linux 8.1 guests.
- Installation of Mandrake Linux 8.0 sometimes hangs at `running /sbin/loader` for no apparent reason. The hang is caused by a bug in early versions of the 2.4 Linux kernel. The bug has been fixed in kernel 2.4.5. Distributions based on this kernel should install without problems.

  For earlier 2.4-series kernels, a workaround is available. Although the Linux kernel bug is not related to CD-ROM drives, the workaround involves changing a GSX Server configuration setting for the virtual DVD/CD-ROM drive.

  Power off the virtual machine and close the GSX Server console window. Open the virtual machine's configuration file (`.vmx` file on a Windows host or `.cfg`

file on a Linux host) in a text editor and add the following line:

```
cdrom.minvirtualtime=100
```

Save the file. Now you should be able to install the guest operating system as described above. After you finish installing the guest operating system, remove this setting from the configuration file, as it may have a performance impact.

Red Hat Enterprise Linux 2.1 Installation Guidelines

The easiest method of installing Red Hat Enterprise Linux AS, ES or WS 2.1 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Enterprise Linux via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: You should not run the X server that is installed when you set up Red Hat Enterprise Linux 2.1. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Enterprise Linux 2.1.

Installation Steps

1. Verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Enterprise Linux 2.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured.
2. Insert the Red Hat Enterprise Linux 2.1 installation CD in the CD-ROM drive on the GSX Server host and power on the virtual machine.

   You need to install Red Hat Enterprise Linux 2.1 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Enterprise Linux 2.1 CD boot prompt, you are offered a number of choices, including the following:

   ```
   To install or upgrade Red Hat Linux ... in graphical mode ...
   To install or upgrade ... in text mode, type: text <ENTER>...
   ...
   Use the function keys listed below ...
   ```

   To choose the text mode installer, type `text` and press Enter.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons** option for three-button mouse support in the virtual machine. If you have a wheel mouse, you may choose **Generic Wheel Mouse (PS/2)**.
5. Choose the language and keyboard, then in the Installation Type screen, choose either **Advanced Server** or **Custom** for the installation type.

6. In the Package Group Selection screen, choose **Software Development** and **Select individual packages**.
7. In the **Individual Package Selection** screen, use the arrow keys to move down to **System Environment/Kernel** and press Enter. Be sure that the following kernels are deselected (no asterisk should appear between the brackets):
   - kernel-enterprise
   - kernel-smp
   - kernel-summit

   Note: VMware has discovered a bug in the Linux kernel supplied with Red Hat Enterprise Linux 2.1 (kernel version 2.4.9-e.3). If you try to boot a kernel configured with SMP support on hardware that does not include a local APIC, the kernel displays a message about dummy APIC emulation and the system hangs later in the boot sequence. This bug affects the kernel-enterprise and kernel-smp packages. The kernel-summit package is specialized for hardware that does not match a GSX Server virtual machine. VMware does not support any of these kernel packages in a virtual machine.
8. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen or partition the virtual disk manually if you do not want to use the Red Hat defaults.
9. You may see a warning that says:
   ```
   The partition table on device sda was unreadable. To
   create new partitions, it must be initialized,
   causing the loss of ALL DATA on the drive.
   Would you like to initialize this drive?
   ```
   This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Yes** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.
10. If your computer is connected to a LAN that provides DHCP support, then in the Network Configuration screen, you may select the **Use bootp/dhcp** option. If you prefer, you may also set the networking parameters manually.
11. In the Video Card Configuration screen, choose **Skip X Configuration**.

This completes basic installation of the Red Hat Enterprise Linux 2.1 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- VMware recommends you do not migrate a Red Hat Enterprise Linux 2.1 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. During the Red Hat Enterprise Linux 2.1 installation, Red Hat Enterprise Linux chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor. Thus, a Red Hat Enterprise Linux 2.1 virtual machine created on a host with an AMD processor may not work if migrated to a host with an Intel processor. The reverse is true; a Red Hat Enterprise Linux 2.1 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

  This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Enterprise Linux 2.1 installation from an AMD machine to an Intel machine, you would experience problems trying to boot from that drive.

Red Hat Linux 9.0 Installation Guidelines

The easiest method of installing Red Hat Linux 9.0 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 9.0 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created and configured a new virtual machine.

Note: You should not run the X server that is installed when you set up Red Hat Linux 9.0. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 9.0.

Installation Steps

1. Insert the Red Hat Linux 9.0 CD-ROM in the CD-ROM drive and power on the virtual machine.

   You need to install Red Hat Linux 9.0 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 9.0 CD boot prompt, you are offered the following choices:

   ```
   To install or upgrade Red Hat Linux ... in graphical mode ...
   To install or upgrade ... in text mode, type: linux text <ENTER>.
   Use the function keys listed below ...
   ```

   To choose the text mode installer, type `linux text` and press Enter.

   Note: If you attempt to use the graphical installer, it fails and launches the text mode installer.

2. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
3. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.
4. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons** option for three-button mouse support in the virtual machine. If you have a wheel mouse, you may choose **Generic Wheel Mouse (PS/2)**.
5. You may see a warning that says:
   `Bad partition table. The partition table on device sda is corrupted. To create new partitions, it must be initialized, causing the loss of ALL DATA on the drive.`

This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.

6. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen or partition the virtual disk manually if you do not want to use the Red Hat defaults.
7. If your computer is connected to a LAN that provides DHCP support, then in the Network Configuration screen, you may select the option **Use bootp/dhcp**. If you prefer, you may also set the networking parameters manually.
8. In the Video Card Configuration screen, choose **Skip X Configuration**.

This completes basic installation of the Red Hat Linux 9.0 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see the manual for your VMware product. Do not start the X server in the guest operating system until you install VMware Tools.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- While installing the Red Hat Linux 9.0 guest operating system, you may notice that the guest performs poorly or slowly, or you may see `INIT` errors when you first boot the guest. To work around this issue and install the guest more easily, pass the `nosysinfo` option when you boot the Linux kernel at the beginning of the installation. At the `boot:` prompt in the guest, type `text nosysinfo`.

  After you install the guest operating system, if you notice that the virtual machine runs slowly or if you still see `INIT` errors, you can modify your boot loader to always use the option when the guest operating system boots. Choose the steps for your boot loader — choose GRUB or LILO.

  Modifying Your GRUB Boot Loader

  A. In a text editor, edit `/etc/grub.conf`.

  B. Look for the following section in the file. Note that you may see a diffrent kernel instead of the 2.4.20-8 kernel shown below.

```
title Red Hat Linux (2.4.20-8)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
    initrd ....
```

C. At the end of the `kernel /vmlinuz-2.4.20-8 ro root=LABEL=/` line, add `nosysinfo`.

D. Save and close the file. You can now boot the guest.

E. Restart the guest operating system.

Note: If you are not confident with changing this configuration file, copy the above four line section and change the title from `Red Hat Linux` to `RH Linux Guest`, and add `nosysinfo` to the end of the line beginning with `kernel` in the newly created section. At boot time, you can choose to boot either the `RH Linux Guest` for optimal performance or `Red Hat Linux` for your original setup.

Modifying Your LILO Boot Loader

A. In a text editor, edit `/etc/lilo.conf`.

B. Look for the following line
`append="....."`

C. Add `nosysinfo` to the line like this:
`append="..... nosysinfo"`

D. If there is no `append=` line in `/etc/lilo.conf`, add the following line:
`append="nosysinfo"`
at the beginning of `/etc/lilo.conf`, before the first `image=` or `other=` directive.

E. Save and close the file.

F. Run the `lilo` command again so your changes can take effect.

G. Restart the guest operating system.

- VMware recommends you do not migrate a Red Hat Linux 9.0 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor.

  During the Red Hat Linux 9.0 installation, Red Hat 9.0 chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor.

Thus, a Red Hat Linux 9.0 virtual machine created on a host with an AMD processor may not work if migrated to a host with an Intel processor. The reverse is also true: a Red Hat Linux 9.0 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Linux 9.0 installation from an AMD machine to an Intel machine, you would experience problems trying to boot from that drive.

Red Hat Linux 8.0 Installation Guidelines

The easiest method of installing Red Hat Linux 8.0 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 8.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: You should not run the X server that is installed when you set up Red Hat Linux 8.0. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 8.0.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 8.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 8.0 installation CD in the CD-ROM drive on your GSX Server host and power on the virtual machine.

   You need to install Red Hat Linux 8.0 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 8.0 CD boot prompt, you are offered the following choices:

   ```
   To install or upgrade Red Hat Linux ... in graphical mode ...
   To install or upgrade ... in text mode, type: linux text <ENTER>.
   Use the function keys listed below ...
   ```

   To choose the text mode installer, type `linux text` and press Enter.

   Note: If you attempt to use the graphical installer, it fails and launches the text mode installer.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons?** option for three-button mouse support in the virtual machine. If you have a wheel mouse, you may choose **Generic Wheel Mouse (PS/2)**.

5. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.
6. You may see a warning that says:
   `Bad partition table. The partition table on device sda is corrupted. To create new partitions, it must be initialized, causing the loss of ALL DATA on the drive.`
   This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.
7. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen or partition the virtual disk manually if you do not want to use the Red Hat defaults.
8. If your host operating system supports DHCP and is connected to a LAN, then in the Network Configuration screen, select the **Use bootp/dhcp** option.
9. In the Video Card Configuration screen, choose **Skip X Configuration**.

This completes basic installation of the Red Hat Linux 8.0 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- VMware recommends you do not migrate a Red Hat Linux 8.0 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. During the Red Hat Linux 8.0 installation, Red Hat 8.0 chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor. Thus, a Red Hat Linux 8.0 virtual machine created on a host with an AMD processor may not work if migrated to a host with an

Intel processor. The reverse is true; a Red Hat Linux 8.0 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Linux 8.0 installation from an AMD machine to an Intel machine, you would experience problems trying to boot from that drive.

Red Hat Linux 7.3 Installation Guidelines

The easiest method of installing Red Hat Linux 7.3 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.3 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: You should not run the X server that is installed when you set up Red Hat Linux 7.3. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.3.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.3 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.3 installation CD in the CD-ROM drive on your GSX Server host and power on the virtual machine.

   You need to install Red Hat Linux 7.3 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.3 CD boot prompt, you are offered the following choices:

   ```
   To install or upgrade a system ... in graphical mode ...
   To install or upgrade a system ... in text mode, type: text <ENTER>.
   To enable expert mode, ...
   Use the function keys listed below ...
   ```

   To choose the text mode installer, type `text` followed by Enter.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons?** option for three-button mouse support in the virtual machine.
5. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.

6. You may see a warning that says:
   ```
   Bad partition table. The partition table on device sda
   is corrupted. To create new partitions, it must be
   initialized, causing the loss of ALL DATA on the
   drive.
   ```
   This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.
7. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen.
8. If your host operating system supports DHCP and is connected to a LAN, then in the Network Configuration screen, select the **Use bootp/dhcp** option.
9. In the Video Card Selection screen, choose any card from the list.
10. In the Video Card Configuration screen, choose **Skip X Configuration**.

This completes basic installation of the Red Hat Linux 7.3 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Note: When you start installing VMware Tools (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Enabling Sound After Installing Red Hat Linux 7.3

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- VMware recommends you do not migrate a Red Hat Linux 7.3 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. During the Red Hat Linux 7.3 installation, Red Hat Linux 7.3 chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor. Thus, a Red Hat Linux 7.3 virtual machine created on a host with an AMD processor may not work if migrated to a host with an Intel processor. The reverse is true; a Red Hat Linux 7.3 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

  This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Linux 7.3 installation from an AMD machine to an Intel machine, you would experience problems trying to boot off that drive.

Red Hat Linux 7.1 and 7.2 Installation Guidelines

The easiest method of installing Red Hat Linux 7.1 or 7.2 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.1 or 7.2 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: You should not run the X server that is installed when you set up Red Hat Linux 7.1 or 7.2. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.1 or 7.2.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.1 or 7.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.1 or 7.2 installation CD in the CD-ROM drive on your GSX Server host and power on the virtual machine.

   You need to install Red Hat Linux 7.1 or 7.2 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.1 or 7.2 CD boot prompt, you are offered the following choices:

   ```
   To install or upgrade a system ... in graphical mode ...
   To install or upgrade a system ... in text mode, type: text <ENTER>.
   To enable expert mode, ...
   Use the function keys listed below ...
   ```

   To choose the text mode installer, type `text` followed by Enter.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.

   A warning appears that says:

   ```
   Bad partition table. The partition table on device sda
   is corrupted. To create new partitions, it must be
   initialized, causing the loss of ALL DATA on the
   ```

`drive.`
This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Click the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.

5. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen.
6. If your host operating system supports DHCP and is connected to a LAN, then in the Network Configuration screen, select the **Use bootp/dhcp** option.
7. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons?** option for three-button mouse support in the virtual machine.
8. In the Video Card Selection screen, choose the default selection.
9. During the configuration of the X server, select the defaults and proceed through this section as quickly as possible, as this X server is replaced by an X server specific to your guest operating system when you install VMware Tools in this virtual machine.
10. Continue to the Starting X screen and click the **Skip** button to skip testing the configuration.

This completes basic installation of the Red Hat Linux 7.1 or 7.2 guest operating system.

VMware Tools
Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing Red Hat Linux 7.1 or 7.2
The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- Installation of Red Hat Linux 7.1 sometimes hangs at `running /sbin/loader` for no apparent reason. The hang is caused by a bug in early versions of the 2.4 Linux kernel. The bug has been fixed in kernel 2.4.5. Distributions based on this kernel should install without problems.

  For earlier 2.4-series kernels, a workaround is available. Although the Linux kernel bug is not related to CD-ROM drives, the workaround involves changing a GSX Server configuration setting for the virtual DVD/CD-ROM drive.

  Power off the virtual machine and close the GSX Server console window. Open the virtual machine's configuration file (`.vmx` file on a Windows host or `.cfg` file on a Linux host) in a text editor and add the following line:

  ```
  cdrom.minvirtualtime=100
  ```

  Save the file. Now you should be able to install the guest operating system as described above. After you finish installing the guest operating system, remove this setting from the configuration file, as it may have a performance impact.
- VMware recommends you do not migrate a Red Hat Linux 7.2 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. During the Red Hat Linux 7.2 installation, Red Hat Linux 7.2 chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor. Thus, a Red Hat Linux 7.2 virtual machine created on a host with an AMD processor may not work if migrated to a host with an Intel processor. The reverse is true; a Red Hat Linux 7.2 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

  This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Linux 7.2 installation from an AMD machine to an Intel machine, you would experience problems trying to boot off that drive.

Red Hat Linux 7.0 Installation Guidelines

The easiest method of installing Red Hat Linux 7.0 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: Due to VGA performance issues installing Red Hat 7.0 with the graphics mode installer, we highly recommend you install the operating system with the text mode installer. At the Red Hat 7.0 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...
To install or upgrade a system ... in text mode, type: text <ENTER>.
To enable expert mode, ...
Use the function keys listed below ...
```

Choose the text mode installer by typing `text` followed by Enter.

Note: During the Red Hat Linux 7.0 text mode installation, a standard XFree86 version 4 server (without support for VMware SVGA or standard VGA) is installed. Do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.0.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.0 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC. Be sure to make the choices outlined in the following steps.
4. In Video Card Selection choose **Generic VGA compatible**, then click **OK**.
5. Near the end of the installation, after files have been copied, you reach the Monitor Setup screen. Choose **Generic Standard VGA, 640x480 @ 60 Hz**, then click **OK**.

6. At the Video Memory screen, choose **256Kb**, then click **OK.**
7. At the Clockchip Configuration screen, choose **No Clockchip Setting (recommended)**, which is the default, then click **OK**.
8. At the Probe for Clocks screen, click **Skip**.
9. At the Select Video Modes screen, don't choose anything. Just click **OK**.
10. At the Starting X screen, click **Skip**.

    Note: This is the most important step. Clicking **OK** runs the XFree86 version 4 server, which fails, and the installer aborts.

This completes basic installation of the Red Hat Linux 7.0 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Installing a 16-Color X Server

If you want to run the standard 16-color VGA X server, skip the installation of VMware Tools and instead take the following steps.

Note: If you use the standard 16-color VGA X server, you do not have the performance advantages of the accelerated SVGA X server included in VMware Tools.

1. After you finish the basic installation of the Red Hat Linux 7.0 guest operating system and the virtual machine reboots, log on as root.

   ```
   su -
   ```

2. Set up the X server:

   ```
   ln -sf ../../usr/X11R6/bin/XF86_VGA16 /etc/X11/X
   ```

   This sets the current X server to `XF86_VGA16` (the XFree86 3.3.6 16-color VGA X server).

Enabling Sound After Installing Red Hat Linux 7.0

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Red Hat Linux 6.x Installation Guidelines

The easiest method of installing Red Hat Linux 6.x in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 6.x via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: Red Hat Linux 6.2 does not run on Pentium 4 processors. It also does not run on Xeon processors that are branded Xeon, with no qualifier, or Xeon-MP (Pentium III Xeon processors are OK).

Note: Due to VGA performance issues installing Red Hat 6.1 and 6.2 with the graphics mode installer, we highly recommend you install the operating system with the text mode installer. At the Red Hat 6.1 or 6.2 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...
To install or upgrade a system ... in text mode, type: text <ENTER>.
To enable expert mode, ...
Use the function keys listed below ...
```

Choose the text mode installer by typing `text` followed by Enter.

Note: During the Red Hat Linux 6.x installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 6.x.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 6.x installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 6.x installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC.

Note: If the virtual machine's Ethernet adapter has been enabled, the installation program auto-detects and loads the AMD PC/Net 32 driver (no command line parameter is necessary to load the driver).

Note: The text mode installer in Red Hat Linux 6.x presents a Hostname Configuration screen. If you are installing this guest with DHCP in a virtual machine with host-only networking, do not specify a host name. Just respond **OK** and continue. (Specifying a host name will cause an installer error later.) At the next screen — Network Configuration — respond **OK** to use the default: **Use bootp/dhcp**.

4. During the Linux installation, select the standard VGA16 X server.
5. In the Choose a Card screen, select the **Generic VGA compatible/Generic VGA** card from the list.
6. In the Monitor Setup screen, select **Generic Monitor** from the list.
7. Select the **Probe** button from the Screen Configuration dialog box.
8. Select **OK** from the Starting X dialog box. After Linux is installed, the generic X server gets replaced with the accelerated X server included in the VMware Tools package when you install VMware Tools.
9. Finish installing Red Hat Linux 6.x as you would on a physical PC.

At this point Red Hat 6.x boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing Red Hat Linux 6.x

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux Enterprise Server 8 Installation Guidelines

The easiest method of installing SuSE Linux Enterprise Server 8 (SLES 8) in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SLES 8 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: During the SLES 8 installation, do **not** install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SLES 8.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SLES 8 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SLES 8 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the text mode installer. In the first installation screen, press the F2 key, then press Enter to select the text mode installer.
5. When prompted, do **not** install an X server. In the Desktop Settings screen, choose Text Mode Only. Click Accept and finish the installation.
6. At the end of the installation, install VMware Tools in your guest operating system. For details, see VMware Tools below.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools and run the SaX2 configuration utility. See Before You Start the X Server below.

Note: When you start installing VMware Tools (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Before You Start the X Server

After you have installed VMware Tools, but before you start the X server, as root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server. If you intend to connect to this virtual machine with the VMware Remote Console, configure the color resolution for 65536 (16-bit) colors or less.

After you run SaX2 you may boot your SLES 8 virtual machine with any of the selections offered in GRUB.

Enabling Sound After Installing SLES 8

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 8.2 Installation Guidelines

The easiest method of installing SuSE Linux 8.2 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 8.2 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created and configured a new virtual machine.

Note: During the SuSE Linux 8.2 installation, do not install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 8.2.

Installation Steps

1. Insert the SuSE Linux 8.2 installation CD in the CD-ROM drive and click the **Power On** button.
2. Follow the installation steps as you would for a physical machine until you get to the selection screens described in the next steps.
3. Install using the text mode installer. In the first installation screen, press the F2 key, type `linux`, then press Enter to select the text mode installer.
4. When prompted, do not install an X server. In the Configure Monitor screen, choose Text Mode Only. Click Accept and finish the installation.

This completes basic installation of the SuSE Linux 8.2 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see the manual for your VMware product. Do not start the X server in the guest operating system until you install VMware Tools and run the SaX2 configuration utility. See Before You Start the X Server on page 315.

Note: When you start installing VMware Tools (by typing `./vmware-install.pl` in the `vmware-tools-distrib` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer Yes to allow the driver to be installed. Answer Yes again to back up the existing video driver files and also copy the

`XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Before You Start the X Server

After you have installed VMware Tools, but before you start the X server, as the root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server.

After you run SaX2 you may boot your SuSE Linux 8.2 virtual machine with any of the selections offered in GRUB.

Known Issues

- On some host systems, the SuSE Linux 8.2 installer attempts to use a kernel that is incompatible with the ACPI features of the virtual hardware. To work around this problem, open the virtual machine's configuration file in a text editor and add the following line:

  ```
  acpi.present = FALSE
  ```

  You should then be able to install and run a SuSE Linux 8.2 guest operating system.
- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 8.1 Installation Guidelines

The easiest method of installing SuSE Linux 8.1 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 8.1 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: During the SuSE Linux 8.1 installation, do **not** install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 8.1.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 8.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 8.1 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the text mode installer. In the first installation screen, press the F2 key, then press Enter to select the text mode installer.
5. SuSE Linux 8.1 installs a PAE-enabled kernel by default on hosts with Pentium 4 processors. To select the non-PAE-enabled kernel, complete the following steps.
   A. Use the arrow keys to select **Software**, then press Enter.
   B. Press Tab until you reach **Detailed Selection**, then press Enter.
   C. Press Tab until you reach **Filter**, then press Enter.
   D. Use the arrow keys to select **RPM Groups**, then press Enter.
   E. Use the arrow keys to select **System**, then press Enter.
   F. Use the arrow keys to select the **k_smp** kernel package, then press the minus key (**-**) to delete it. Press Enter to confirm the deletion.

G. Use the arrow keys to select the **k_dflt** kernel package, then press the plus key (+) to select it. Press Enter to confirm the selection.

H. Press Tab until you reach **OK**, then press Enter.

I. Press Tab until you reach **Accept**, then press Enter to continue the installation.

6. When prompted, do **not** install an X server. In the Configure Monitor screen, choose Text Mode Only. Click Accept and finish the installation.
7. At the end of the installation, install VMware Tools in your guest operating system. For details, see VMware Tools below.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools and run the SaX2 configuration utility. See Before You Start the X Server below.

Note: When you start installing VMware Tools (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Before You Start the X Server

After you have installed VMware Tools, but before you start the X server, as root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server. If you intend to connect to this virtual machine with the VMware Remote Console, configure the color resolution for 65536 (16-bit) colors or less.

After you run SaX2 you may boot your SuSE Linux 8.1 virtual machine with any of the selections offered in GRUB.

Enabling Sound After Installing SuSE Linux 8.1

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 8.0 Installation Guidelines

The easiest method of installing SuSE Linux 8.0 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 8.0 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: During the SuSE Linux 8.0 installation, do **not** install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 8.0.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 8.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 8.0 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the text mode installer.
5. SuSE Linux 8.0 installs a PAE-enabled kernel by default. To select the non-PAE-enabled kernel, complete the following steps.
   A. Use the arrow keys to select **Software**, then press Enter.
   B. Press Tab until you reach **Detailed Selection**, then press Enter.
   C. Press Tab until you reach **Select Single Packages**, then press Enter.
   D. Press Tab until you reach **Show Package Sets**, then press the spacebar to mark the selection.
   E. Press Tab until you reach the **Set Description** box.
   F. Use the arrow keys to select **Installable Kernels**, then press Enter.
   G. Press Tab until you reach the **k_i386** kernel package, then press the spacebar to mark the k_i386 kernel selection.

H. Press Tab until you reach **OK**, then press Enter to continue the installation.

6. When prompted, do **not** install an X server. In the Configure Monitor screen, choose No X11. The installer asks you to confirm. Click Continue and finish the installation.
7. At the end of the installation, install VMware Tools in your guest operating system. For details, see VMware Tools below.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools and run the SaX2 configuration utility. See Before You Start the X Server below.

Note: When you start installing VMware Tools (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Before You Start the X Server

After you have installed VMware Tools, but before you start the X server, as root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server.

After you run SaX2 you may boot your SuSE Linux 8.0 virtual machine with any of the selections offered in LILO.

Enabling Sound After Installing SuSE Linux 8.0

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux Enterprise Server 7 Installation Guidelines

The easiest method of installing SuSE Linux Enterprise Server 7 (SLES 7) in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SLES 7 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the GSX Server New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SLES 7 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SLES 7.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SLES 7 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SLES 7 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next step.
4. Part way through the installation, the installer reboots the virtual machine. At the LILO screen, let the boot proceed using the default selection of `linux`.
5. At the Desktop Settings screen, select **640x480 256 colors**.
6. Finish installing SLES 7 as you would on a physical machine.
7. At the end of the installation, install VMware Tools in your guest operating system. For details, see VMware Tools below.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing SLES 7

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 7.3 Installation Guidelines

The easiest method of installing SuSE Linux 7.3 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.3 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: During the SuSE Linux 7.3 installation, do **not** install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.3.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.3 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.3 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the text mode installer.
5. When prompted, do **not** install an X server. In the Configure Monitor screen, choose No X11. The installer asks you to confirm. Click **Continue** and finish the installation.
6. At the end of the installation, install VMware Tools in your guest operating system. For details, see VMware Tools below.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools and run the SaX2 configuration utility. See Before You Start the X Server on page 325.

Before You Start the X Server

After you have installed VMware Tools, but before you start the X server, as root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server.

After you run SaX2 you may boot your SuSE Linux 7.3 virtual machine with any of the selections offered in LILO.

Enabling Sound After Installing SuSE Linux 7.3

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 7.2 Installation Guidelines

The easiest method of installing SuSE Linux 7.2 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.2 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 7.2 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.2.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.2 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the text mode installer.
5. At the Desktop Settings screen, select **640x480 256 colors**.
6. Finish installing SuSE Linux 7.2 as you would on a physical machine.

VMware Tools

At the end of the installation, boot again using the default LILO selection of `linux`, then install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools and, if you used the text installer, run the SaX2 configuration utility. See Before You Start the X Server on page 325.

After you have installed VMware Tools, you may boot your SuSE 7.2 virtual machine with any of the selections offered in LILO.

Before You Start the X Server

If you used the text installer, then after you have installed VMware Tools, but before you start the X server, as root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server.

After you run SaX2 you may boot your SuSE Linux 7.2 virtual machine with any of the selections offered in LILO.

Enabling Sound After Installing SuSE Linux 7.2

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 7.1 Installation Guidelines

The easiest method of installing SuSE Linux 7.1 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.1 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 7.1 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.1.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.1 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Use the graphical installer and follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next step.
4. You are offered a choice of Linux kernels to install. Kernel 2.2.18 is selected by default. Be sure to leave it selected. If you want to use kernel 2.4 in your virtual machine, select both.
5. Part way through the installation, the installer reboots the virtual machine. At the LILO screen, let the boot proceed using the default selection of `linux` to use the 2.2.18 kernel.
6. At the Desktop Settings screen, select **640x480 256 colors**.
7. Finish installing SuSE Linux 7.1 as you would on a physical machine.

VMware Tools

At the end of the installation, boot again using the default LILO selection of `linux`, then install VMware Tools in your guest operating system. For details, see Installing

VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

After you have installed VMware Tools, you may boot your SuSE Linux 7.1 virtual machine with any of the selections offered in LILO.

Caution: If you selected No X11 during the installation, you must create a link to the X server before you can start it. After you finish installing VMware Tools, in the guest operating system, open a terminal and type the following commands:

```
cd /
su -
mv /var/X11R6/bin/X /usr/X11R6/bin/XF86-Xserver
ln -s /usr/X11R6/bin/XF86-Xserver /var/X11R6/bin/X
ln -s /etc/XF86Config-4 /etc/XF86Config
```

Enabling Sound After Installing SuSE Linux 7.1

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- When you are installing SuSE Linux 7.1 in text mode and the guest operating system reboots for the first time, the display turns completely black and the guest appears to be hung.

  Despite its appearance, the guest operating system actually is not hung; instead, the screen is not being displayed. To see the screen and continue with the installation, in the guest operating system, switch to Linux virtual console 2. Press Ctrl-Alt, press and release the spacebar, then press F2.

  Then return to virtual console 1. Press Ctrl-Alt, press and release the spacebar, then press F1. You should be able to see the screen and continue installing the guest operating system.

  Note: If you are using a different hot-key combination, use that in place of Ctrl-Alt above.

  Note: This problem appears only when you install the guest operating system in text mode.

SuSE Linux 7.0 Installation Guidelines

The easiest method of installing SuSE Linux 7.0 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 7.0 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.0.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. Be sure the virtual machine's memory is set to at least 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.0 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Use the graphical installer and follow the installation steps as you would for a physical machine.
4. In the Desktop Settings screen, select **640x480 256 colors**.
5. Finish installing SuSE Linux 7.0 as you would on a physical machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing SuSE Linux 7.0

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- When you are installing SuSE Linux 7.0 in text mode and the guest operating system reboots for the first time, the display turns completely black and the guest appears to be hung.

  Despite its appearance, the guest operating system actually is not hung; instead, the screen is not being displayed. To see the screen and continue with the installation, in the guest operating system, switch to Linux virtual console 2. Press Ctrl-Alt, press and release the spacebar, then press F2.

  Then return to virtual console 1. Press Ctrl-Alt, press and release the spacebar, then press F1. You should be able to see the screen and continue installing the guest operating system.

  Note: If you are using a different hot-key combination, use that in place of Ctrl-Alt above.

  Note: This problem appears only when you install the guest operating system in text mode.

SuSE Linux 6.3 and 6.4 Installation Guidelines

The easiest method of installing SuSE Linux 6.3 or 6.4 in a virtual machine is to use the standard SuSE distribution CDs. Be sure that you boot from CD No. 2 (the "expert install" CD), not CD No. 1. (The installer on CD No. 1 is designed for SVGA. Until you install VMware Tools, as described below, the virtual machine supports only VGA graphics. This makes it impossible for you to see some of the choices you must make during the installation.)

The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 6.3 or 6.4 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 6.3 or 6.4 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 6.3 or 6.4.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 6.3 or 6.4 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert SuSE Linux 6.3 or 6.4 installation CD No. 2 in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC, until you get to the selection screens described in the next step.

   Note: Part way through the process, the installer asks you to insert CD number 1, even if you initially booted from CD number 2. You should, indeed, insert CD number 1 at that point. When the installer asks, "Which type of install do you prefer: Text or Graphical," be sure to choose text.
4. If you have Ethernet configured, a pop-up message appears stating that the `pcnet32` driver is loaded automatically. The driver's long name is displayed as AMD PCI PCnet32 (PCI bus NE2100).

5. From the Installation – YaST screen, select the packages you want to install and select the **Start Installation** option to continue.
6. Finish installing SuSE Linux 6.3 or 6.4 as you would on a physical PC.

At this point SuSE Linux 6.3 or 6.4 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing SuSE Linux 6.3 or 6.4

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 6.2 Installation Guidelines

The easiest method of installing SuSE Linux 6.2 in a virtual machine is to use the standard SuSE distribution CD. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 6.2 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 6.2 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 6.2.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 6.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 6.2 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC, until you get to the selection screens described in the next step.
4. If you have Ethernet configured, a pop-up message appears stating that the `pcnet32` driver is loaded automatically. The driver's long name is displayed as AMD PCI PCnet32 (PCI bus NE2100).
5. From the Installation – YaST screen, select the packages you want to install and select the **Start Installation** option to continue.
6. Finish installing SuSE Linux 6.2 as you would on a physical PC.

At this point SuSE Linux 6.2 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing SuSE Linux 6.2

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 6.1 Installation Guidelines

The easiest method of installing SuSE Linux 6.1 in a virtual machine is to use the standard SuSE distribution CD. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 6.1 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 6.1 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 6.1.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 6.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 6.1 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. If the virtual machine's Ethernet adapter has been enabled, you must configure Linux to load the appropriate driver. Select **Kernel Modules (Hardware Drivers)** from the install program's main menu, then select **Autoload of Modules**. A pop-up message appears stating that the `pcnet32` driver will be loaded automatically. The driver's long name is displayed as AMD PCI PCnet32 (PCI bus NE2100).
4. Follow the installation steps as you would for a physical PC, until you get to the selection screen described in the next step.
5. From the Installation – YaST screen, select the packages you want to install and select the **Start Installation** option to continue.

   Note: If you want the virtual machine to use DHCP to get its IP address, verify that the `dhclient` package is selected before selecting **Start Installation**.

   A. Choose the **Change/Create Configuration** option.

   B. Press the F4 key and select **All Packages** from the pop-up dialog box.

C. Select **All Packages (Excluding Sources)** and verify that the `dhclient` package is selected in the Package Selection screen.

6. Finish installing SuSE Linux 6.1 as you would on a physical PC.

At this point SuSE Linux 6.1 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing SuSE Linux 6.1

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 6.0 Installation Guidelines

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Refer to the SuSE Linux 6.0 manual during the installation. Remember that you can run only the Standard VGA16 X server until you install VMware Tools, which includes an accelerated SVGA X server.

Networking Notes

SuSE Linux 6.0 does not install the DHCP client as a default. You should select this package if you wish to use DHCP with your virtual machine. Otherwise you must allocate a static IP address for the virtual machine.

When prompted to select the network card, select the AMD PCI PCnet32 (PCI bus NE2100).

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing SuSE Linux 6.0

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Turbolinux 7.0 Installation Guidelines

The easiest method of installing Turbolinux 7.0 in a virtual machine is to use the standard Turbolinux 7.0 distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Turbolinux 7.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Turbolinux 7.0 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing Turbolinux 7.0, before you start the X server.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Turbolinux 7.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Turbolinux 7.0 installation CD #1 in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC, until you get to the selection screen described in the next step.
4. In the Configure Monitor screen, follow the defaults to configure an X server. This is necessary even though you will install a different X server with VMware Tools after you finish installing the guest operating system.
5. Finish installing Turbolinux 7.0 as you would on a physical PC.

At this point Turbolinux 7.0 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Note: If you plan to test scripts in a Turbolinux 7.0 guest operating system, you need to update the Turbolinux guest operating system. This is a known issue with Turbolinux. Go to

ftp://ftp.turbolinux.com/pub/turbolinux-updates/7.0/RPMS/initscripts-7.0.0-18.i586.rpm. For more information about running scripts in a guest operating system, see Executing Scripts When the Virtual Machine's Power State Changes on page 122.

Enabling Sound After Installing Turbolinux 7.0

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Turbolinux 6.0 Installation Guidelines

The easiest method of installing Turbolinux 6.0 in a virtual machine is to use the standard Turbolinux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Turbolinux 6.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: Do not install Turbolinux 6.0 on a Pentium 4 host.

Note: During the Turbolinux 6.0 installation, a standard VGA16 X server (without support for the GSX Server X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing Turbolinux 6.0.

Installation Steps

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Turbolinux 6.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Turbolinux 6.0 installation CD in the CD-ROM drive on your GSX Server host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC, until you get to the selection screens described in the next steps.
4. In the Configure Video Card screen, select the defaults for the X server.
5. In the Configure X Server screen, click **Skip**. You must not configure this X server. When you install VMware Tools, an X server is installed that is optimized for running in your virtual machine.
6. Finish installing Turbolinux 6.0 as you would on a physical PC.

At this point Turbolinux 6.0 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Enabling Sound After Installing Turbolinux 6.0

The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**) after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in GSX Server on page 475.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

NetWare 6.0 and 6.5 Server Installation Guidelines

You can install NetWare 6.0 in a virtual machine using the standard Novell NetWare 6.0 CD-ROM.

You can install NetWare 6.5 in a virtual machine using the standard Novell NetWare 6.5 Operating System and Product CD-ROMs.

VMware recommends you install NetWare on a host with at least 384MB of memory.

Preparing Your GSX Server Linux Host

If you are going to create and run this NetWare virtual machine on a Linux host, change the host's color depth to 256 colors/8-bit color before you create the virtual machine and install the guest operating system.

Creating and Configuring the NetWare Virtual Machine

1. Create a virtual machine configuration with the New Virtual Machine Wizard (Windows host) or Configuration Wizard (Linux host). For the most part, you can choose your own settings, except as noted below.
   A. For the type of configuration, select **Typical**.
   B. For the guest operating system, select **NetWare 6**.
   C. Keep the memory setting for the virtual machine at its default of 512MB.
   D. Create a new **IDE** virtual disk no smaller than the default of 4GB in size.
2. If you created this virtual machine on a Linux host, open the configuration file (`<netware>.cfg`) in a text editor and add the following line:
   `gui.iconLEDS = false`
   This removes all the LED icons in the console window, which prevents the virtual machine display from appearing incorrectly when you power it on while the host is in 8 bit/256 color mode.
3. Next, install the guest operating system and VMware Tools, which includes the CPU idler program. See below for details.

Installing the Guest Operating System

To install NetWare 6.0 or 6.5 in a virtual machine, complete the following steps.

1. Begin installing the guest operating system. Insert the Novell NetWare 6.0 installation CD or NetWare 6.5 Product CD into the CD-ROM drive on your GSX Server host and power on the virtual machine.
2. Read and accept the license agreement.

Note: If you are installing NetWare 6.5, a few prompts appear before you reach the license agreement. Accept the defaults for installing NetWare, the CD-ROM drive type, how to restore the floppy drive and the run mode, then continue.

3. When prompted, choose **IDE CD-ROM**.
4. Create a new boot partition. The guest operating system reboots. The installation continues.
5. To configure IP networking, do one of the following:
   - If you chose bridged networking for the virtual machine, enter its IP address.

     Note: On a Windows NT host, when NetWare tries to load the LAN driver (using `pcntnw.lan`), it fails because it broadcasts for its own IP address. This causes IP networking to fail.

     To work around this, open the System Console (press Ctrl-Esc) and type
     `set allow ip address duplicates=on`

     Press Alt-Esc to return to the installation.
   - If you chose host-only networking for the virtual machine, look up the host machine's IP address.

     At a command prompt on a Windows host, type
     `ipconfig /all`

     At a command prompt on a Linux host, type
     `ifconfig`

     Note the host's IP address for VMnet1 and change the last octet so it is greater than the last octet in the IP address of the host.

     For example, if the host IP address is 192.168.160.1, then the virtual machine's IP address is 192.168.160.###, where ### is any number greater than 1 and less than 128.

     For the subnet mask, enter 255.255.255.0.

     For the router gateway, enter the host's IP address (192.168.80.1 in our example).
   - If you chose network address translation (NAT) for the virtual machine, look up the host machine's IP address.

     At a command prompt on a Windows host, type
     `ipconfig /all`

     At a command prompt on a Linux host, type
     `ifconfig`

Note the host's IP address for VMnet8 and change the last octet so it is greater than the last octet in the IP address of the host.

For example, if the host IP address is 192.168.160.1, then the virtual machine's IP address is 192.168.160.###, where ### is any number greater than 2 and less than 128.

For the subnet mask, enter 255.255.255.0.

For the router gateway, enter the NAT service's IP address (192.168.80.2 in our example).

Note that with Network Address Translation, there are 2 IP addresses in use on the host:

* The IP address assigned to the interface for VMnet8 (which shows up in the `ipconfig` output with a ".1" in the last octet).

* The IP address used by the NAT device itself (which always uses ".2" as the last octet).

6. Finish the installation by following the on-screen instructions.

   After you finish the installation, install VMware Tools, which installs and loads the CPU idler program.

VMware Tools for NetWare 6.0 or 6.5 Guest Operating Systems

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Installing VMware Tools also installs and loads the CPU idler program. NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy. To prevent unnecessary slowdowns, VMware recommends that, after you install VMware Tools, you keep the NetWare CPU idle program loaded.

NetWare 6.5 Known Issues

- Whenever you reboot the guest operating system, it can take up to six minutes before you can regain control of the keyboard or mouse.
- If you are using text mode and want to browse the file system, you may notice that the arrow keypad and Insert key do not allow you to navigate directories. To work around this issue, use the numeric keypad, but first turn off the number lock by pressing the Num Lock key.

NetWare 6.0 Known Issues

- After the virtual machine reboots while installing VMware Tools, make sure the virtual machine releases the VMware Tools ISO image. Choose **Devices** > **<CD-ROM>**, and if the CD-ROM's submenu shows the VMware Tools ISO image, choose **Disconnect**.
- The VMware Tools feature that synchronizes the time in the guest operating system with the time in the host operating system does not work with NetWare 6.0. This issue may be resolved in the next NetWare 6.0 support pack that Novell will release.
- If you are using text mode and want to browse the file system, you may notice that the arrow keypad and Insert key do not allow you to navigate directories. To work around this issue, use the numeric keypad, but first turn off the number lock by pressing the Num Lock key.
- During the installation of the guest operating system, if you get an `ABEND` error in the `JVM.NLM` module, try installing the operating system again. This is a third party problem that occurs rarely, but when it does, it occurs during installation only. Once you complete the installation, you should not see this error again.
- If you installed NetWare 6.0 Support Pack 2 in your guest operating system, you cannot mount CD-ROMs. To mount a CD-ROM with the support pack installed, do one of the following:
  - Set the primary hard drive to IDE 0:0 and the CD-ROM drive to IDE 0:1.
  - Copy the original driver files (`IDEATA.DDI` and `IDEATA.HAM`) from the `Drivers\Storage` directory of the installation CD-ROM that shipped with NetWare 6.0 to the `c:\nwserver` directory.
  - Scan for new devices. In the System Console, type
    ```
    scan for new devices
    ```
    Then load the CD-ROM. In the System Console, type:
    ```
    load cd9660.nss
    ```

  Note: If you cannot mount CD-ROMs, you cannot install VMware Tools in the virtual machine.

NetWare 5.1 Server Installation Guidelines

You can install NetWare 5.1 in a virtual machine using the standard Novell NetWare 5.1 CD-ROM. VMware recommends you install NetWare 5.1 on a host with at least 384MB of memory.

Preparing Your GSX Server Linux Host

If you are going to create and run this NetWare virtual machine on a Linux host, change the host's color depth to 256 colors/8-bit color before you create the virtual machine and install the guest operating system.

Creating and Configuring the NetWare Virtual Machine

1. Create a virtual machine configuration with the New Virtual Machine Wizard (Windows host) or Configuration Wizard (Linux host). For the most part, you can choose your own settings, except as noted below.
   A. For the type of configuration, select **Typical**.
   B. For the guest operating system, select **NetWare 5**.
   C. Keep the memory setting for the virtual machine at its default of 512MB.
   D. Create a new **IDE** virtual disk no smaller than the default of 4GB in size.
2. If you created this virtual machine on a Linux host, open the configuration file (`<netware>.cfg`) in a text editor and add the following line:
   `gui.iconLEDS = false`
   This removes all the LED icons in the console window, which prevents the virtual machine display from appearing incorrectly when you power it on while the host is in 8 bit/256 color mode.
3. Next, install the guest operating system and VMware Tools, which includes the CPU idler program. See below for details.

Installing the Guest Operating System

To install NetWare 5.1 in a virtual machine, complete the following steps.

1. Insert the Novell NetWare 5.1 installation CD into the CD-ROM drive on your GSX Server host and power on the virtual machine.
2. Read and accept the license agreement.
3. Create a new boot partition. The guest operating system reboots. The installation continues.
4. To configure IP networking, do one of the following:
   - If you chose bridged networking for the virtual machine, enter its IP address.

Note: On a Windows NT host, when NetWare tries to load the LAN driver (using `pcntnw.lan`), it fails because it broadcasts for its own IP address. This causes IP networking to fail.

To work around this, open the System Console (press Ctrl-Esc) and type
`set allow ip address duplicates=on`

Press Alt-Esc to return to the installation.

- If you chose host-only networking for the virtual machine, look up the host machine's IP address.

  At a command prompt on a Windows host, type
  `ipconfig /all`

  At a command prompt on a Linux host, type
  `ifconfig`

  Note the host's IP address for VMnet1 and change the last octet so it is greater than the last octet in the IP address of the host.

  For example, if the host IP address is 192.168.160.1, then the virtual machine's IP address is 192.168.160.###, where ### is any number greater than 1 and less than 128.

  For the subnet mask, enter 255.255.255.0.

  For the router gateway, enter the host's IP address (192.168.80.1 in our example).

- If you chose network address translation (NAT) for the virtual machine, look up the host machine's IP address.

  At a command prompt on a Windows host, type
  `ipconfig /all`

  At a command prompt on a Linux host, type
  `ifconfig`

  Note the host's IP address for VMnet8 and change the last octet so it is greater than the last octet in the IP address of the host.

  For example, if the host IP address is 192.168.160.1, then the virtual machine's IP address is 192.168.160.###, where ### is any number greater than 2 and less than 128.

  For the subnet mask, enter 255.255.255.0.

  For the router gateway, enter the NAT service's IP address (192.168.80.2 in our example).

Note that with Network Address Translation, there are 2 IP addresses in use on the host:

* The IP address assigned to the interface for VMnet8 (which shows up in the `ipconfig` output with a ".1" in the last octet).

* The IP address used by the NAT device itself (which always uses ".2" as the last octet).

5. Finish the installation by following the on-screen instructions.

   After you finish the installation, install VMware Tools, which installs and loads the CPU idler program.

VMware Tools for NetWare 5.1 Guest Operating Systems

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113.

Installing VMware Tools also installs and loads the CPU idler program. NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy. To prevent unnecessary slowdowns, VMware recommends that, after you install VMware Tools, you keep the NetWare CPU idle program loaded.

Known Issues

- After the virtual machine reboots while installing VMware Tools, make sure the virtual machine releases the VMware Tools ISO image. Choose **Devices** > **<CD-ROM>**, and if the CD-ROM's submenu shows the VMware Tools ISO image, choose **Disconnect**.
- During the installation of the guest operating system on an Intel Pentium 4 host, you may encounter a Page Fault error. If this error occurs, you must apply a NetWare 5.1 patch on the host machine. For details, see *support.novell.com/cgi-bin/search/searchtid.cgi?/2958220.htm*.
- If you are using text mode and want to browse the file system, you may notice that the arrow keypad and Insert key do not allow you to navigate directories. To work around this issue, use the numeric keypad, but first turn off the number lock by pressing the Num Lock key.
- If you installed NetWare 5.1 Support Pack 5 in your guest operating system, you cannot mount the CD-ROM. To mount a CD-ROM with the support pack installed, do one of the following:
  - Set the primary hard drive to IDE 0:0 and the CD-ROM drive to IDE 0:1.

- Copy the original driver files (`IDEATA.DDI` and `IDEATA.HAM`) from the `Drivers\Storage` directory of the installation CD-ROM that shipped with NetWare 5.1 to the `c:\nwserver` directory.

Note: If you cannot mount CD-ROMs, you cannot install VMware Tools in the virtual machine.

NetWare 4.2 Server Installation Guidelines

You can install NetWare 4.2 in a virtual machine using the standard Novell NetWare 4.2 installation CD. VMware recommends you install NetWare 4.2 on a host with at least 256MB of memory.

Preparing Your GSX Server Linux Host

If you are going to create and run this NetWare virtual machine on a Linux host, change the host's color depth to 256 colors/8-bit color before you create the virtual machine and install the guest operating system.

Creating and Configuring the NetWare Virtual Machine

1. Create a virtual machine configuration with the New Virtual Machine Wizard (Windows host) or Configuration Wizard (Linux host). For the most part, you can choose your own settings, except as noted below.
   A. For the type of configuration, select **Custom**.
   B. For the guest operating system, select **NetWare 4**.
   C. Allocate 128MB of memory for the virtual machine.
   D. Create a new **IDE** virtual disk no smaller than the default of 4GB in size.
2. If you created this virtual machine on a Linux host, open the configuration file (`<netware>.cfg`) in a text editor and add the following line:
   `gui.iconLEDS = false`
   This removes all the LED icons in the console window, which prevents the virtual machine display from appearing incorrectly when you power it on while the host is in 8 bit/256 color mode.
3. Next, install the guest operating system and VMware Tools, which includes the CPU idler program. See below for details.

Installing the Guest Operating System

To install NetWare 4.2 in a virtual machine, complete the following steps.

1. Use the GSX Server Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, be sure that your virtual machine is configured for at least 48MB of memory (which the NetWare server installation requires). VMware also recommends that you disable the screen saver on the host before starting the installation process.
2. VMware recommends that you install MS-DOS 5.0 or higher in a small (50MB FAT16) partition as described in these guidelines. The rest of the free space on the virtual disk is used for the NetWare partition. Even if the virtual machine is to

run NetWare most of the time, it is a good idea to install the `DOSIDLE.EXE` program, which you can download from *www.vmware.com/software/dosidle210.zip*.

3. Install a CD-ROM driver or CD-ROM software for DOS. If you have problems setting up the DOS virtual machine to access the CD-ROM drive, you can use the `mtmcdai.sys` driver, which can be found at *www.mitsumi.com*. Under **Drivers and Manuals** look for `ide158.exe`. Modify the `config.sys` and `autoexec.bat` files on your DOS boot floppy (along with the `mscdex.exe` file) as shown below. If you are using a DOS boot partition, adjust the drive letters accordingly.

   ```
   config.sys

   device=himem.sys /testmem:off
   device=NEC_IDE.SYS /D:MSCD001
   files=12
   buffers=15
   stacks=9,256
   lastdrive=z


   autoexec.bat

   @ECHO OFF
   set EXPAND=YES
   SET DIRCMD=/O:N
   cls
   set temp=c:\
   set tmp=c:\
   path=c:\

   IF "%config%"=="NOCD" GOTO QUIT
   a:\NWCDEX.EXE /D:mscd001

   :QUIT
   ```

   After you have configured the CD-ROM software, verify that the virtual machine can read a CD from the host system's CD-ROM drive.

4. If the virtual machine is not running, power it on and wait for DOS finish its boot process.

5. Insert the NetWare 4.2 CD in the CD-ROM drive on the GSX Server host.

6. In the virtual machine, at the DOS prompt, run `fdisk` to create a partition for NetWare.
   ```
   A:\>fdisk
   ```
7. After you create the partition, reboot the virtual machine. Press Ctrl-Alt-Insert.
8. Format the C: drive. Type the following:
   ```
   A:\>format c: /s /x
   ```
9. Copy the following files to your C: drive from your floppy. Type the following:
   ```
   A:\>Copy autoexec.bat c:
   A:\>Copy config.sys c:
   A:\>Copy himem.sys c:
   A:\>Copy nwcdex.exe c:
   A:\>Copy nec_ide.sys c:
   ```
10. Modify the `autoexec.bat` file so it points to the CD-ROM directory on the hard drive instead of the floppy drive.
    A. To modify autoexec.bat, type the following:
       ```
       C:\>a:edit autoexec.bat
       ```
    B. The line
       ```
       a:\NWCDEX.EXE /D:mscd001
       ```
       Must be changed to
       ```
       c:\NWCDEX.EXE /D:mscd001
       ```
    C. Save the changes you just made.
       ```
       C:\>cd d:
       ```
11. Run `INSTALL.BAT` to start the NetWare server installation process. Install the software in a virtual machine as you would for a physical PC.
12. If the virtual machine has been configured for networking (bridged, host-only, NAT or custom), the installation program detects a PCI Ethernet adapter and prompts you with a list of possible drivers. At this point, do not select or load any LAN drivers; press the F3 key to continue installing without a LAN driver.

    Note: Once the installation has been completed, you can load and bind the appropriate LAN driver. Selecting or loading a LAN driver during the NetWare 4.2 installation may hang the installation process.
13. Finish the NetWare 4.2 installation by following the on-screen instructions.

    Then shut down the server and type `exit` to return to a DOS prompt.

    After you finish the installation, install VMware Tools, which installs and loads the CPU idler program.

VMware Tools for NetWare 4.2 Guest Operating Systems

Be sure to install VMware Tools in your guest operating system. In NetWare 4.2 virtual machines, VMware Tools provides CPU idling, sends a heartbeat from the guest operating system to the host and gives the virtual machine the ability to be gracefully powered on or off. See Installing VMware Tools on page 113.

Installing VMware Tools also installs and loads the CPU idler program. NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy. To prevent unnecessary slowdowns, VMware recommends that, after you install VMware Tools, you keep the NetWare CPU idle program loaded.

FreeBSD Installation Guidelines

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Various versions and distributions of FreeBSD have been tested with the current GSX Server distribution. The 3.x and 4.0 through 4.5 distributions of FreeBSD — specifically 3.1, 4.0, 4.1, 4.2, 4.3, 4.4 and 4.5 — are fully functional. Floppy, CD-ROM and network devices autoconfigure and work.

Setting the Disk Geometry for a FreeBSD SCSI Virtual Disk

Versions of FreeBSD older than 4.4 do not boot if the operating system has been installed on a 2GB or larger SCSI virtual disk. To correct this issue, you need to set the disk geometry for the SCSI virtual disk or use IDE disks.

FreeBSD fails to boot because the virtual disk geometry is not probed correctly by FreeBSD when you install the guest operating system. FreeBSD installs the boot loader in the wrong location on the virtual disk. When FreeBSD tries to boot, the FreeBSD boot loader asks the BIOS for important data that is now on a different section of the virtual disk, so FreeBSD cannot boot.

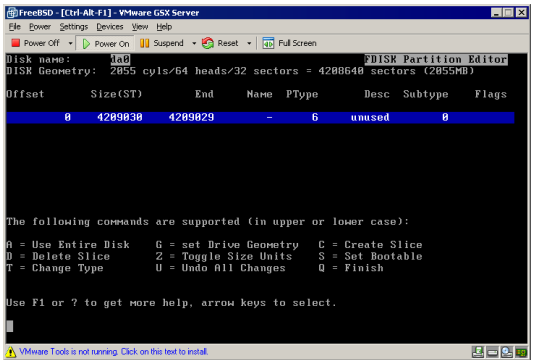
This problem has been fixed in FreeBSD 4.4. This and later versions correctly boot SCSI virtual disks of any size.

To use an older version of FreeBSD in your virtual machine, you can do one of two things:

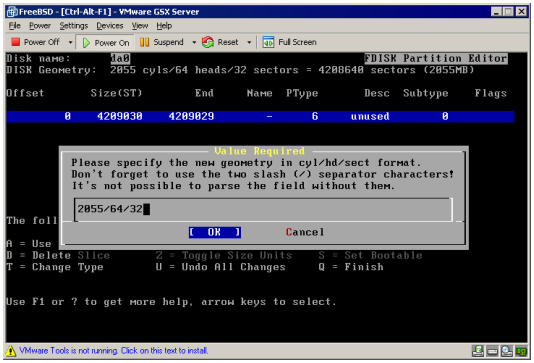
- Use an IDE virtual disk in your virtual machine. You may need to add the IDE virtual disk to the virtual machine with the Configuration Editor.
- Set the disk geometry by hand when installing FreeBSD in a SCSI virtual disk. These steps are outlined below.

To set the disk geometry manually, complete these steps.

1. FreeBSD calculates an incorrect disk geometry before you arrive at the FDISK Partition Editor, as illustrated here.


FreeBSD - [Ctrl-Alt-F1] - VMware GSX Server
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
Disk name: da0 FDISK Partition Editor
DISK Geometry: 2055 cyls/64 heads/32 sectors = 4208640 sectors (2055MB)
Offset Size(ST) End Name PType Desc Subtype Flags
0 4209030 4209029 - 6 unused 0
The following commands are supported (in upper or lower case):
A = Use Entire Disk G = set Drive Geometry C = Create Slice
D = Delete Slice Z = Toggle Size Units S = Set Bootable
T = Change Type U = Undo All Changes Q = Finish
Use F1 or ? to get more help, arrow keys to select.
VMware Tools is not running. Click on this text to install.

2. To set the disk geometry, press G to select the Set Drive Geometry option. A dialog box appears, containing numbers like 2055/64/32, representing the incorrect geometry in cylinders, heads and sectors per head.

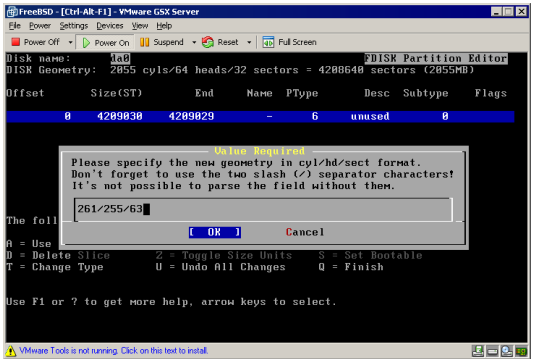

FreeBSD - [Ctrl-Alt-F1] - VMware GSX Server
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
Disk name: da0 FDISK Partition Editor
DISK Geometry: 2055 cyls/64 heads/32 sectors = 4208640 sectors (2055MB)
Offset Size(ST) End Name PType Desc Subtype Flags
0 4209030 4209029 - 6 unused 0
Value Required
Please specify the new geometry in cyl/hd/sect format.
Don't forget to use the two slash (/) separator characters!
It's not possible to parse the field without them.
2055/64/32
[OK] Cancel
A = Use
D = Delete Slice Z = Toggle Size Units S = Set Bootable
T = Change Type U = Undo All Changes Q = Finish
Use F1 or ? to get more help, arrow keys to select.
VMware Tools is not running. Click on this text to install.

3. To calculate the correct geometry, find the total number of sectors by multiplying the number of cylinders, heads and sectors per head together, then dividing the number of sectors by the correct number of heads and sectors per head.

   In the above illustration, the virtual disk is a 2055MB disk with 2055 cylinders, 64 heads and 32 sectors per head (these numbers represent the incorrect

geometry). The product of these three numbers (2055 x 64 x 32) equals 4,208,640 sectors.

To determine the correct geometry for the BusLogic compatible virtual SCSI adapter used by GSX Server, calculate the number of cylinders, which is 4,208,640 sectors divided by the product of the actual number of heads and sectors per head (255 heads times 63 sectors per head). This results in a total of 261 actual cylinders (4208640/(255 * 63) = 261, rounded down).


FreeBSD - [Ctrl-Alt-F1] - VMware GSX Server
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
Disk name: da0 FDISK Partition Editor
DISK Geometry: 2055 cyls/64 heads/32 sectors = 4208640 sectors (2055MB)
Offset Size(ST) End Name PType Desc Subtype Flags
0 4209030 4209029 - 6 unused 0
Value Required
Please specify the new geometry in cyl/hd/sect format.
Don't forget to use the two slash (/) separator characters!
It's not possible to parse the field without them.
261/255/63
[OK] Cancel
The foll
A = Use
D = Delete Slice Z = Toggle Size Units S = Set Bootable
T = Change Type U = Undo All Changes Q = Finish
Use F1 or ? to get more help, arrow keys to select.
VMware Tools is not running. Click on this text to install.

4. You can now enter the correct geometry of 261 cylinders, 255 heads and 63 sectors per head by typing `261/255/63` in the dialog box. Then click **OK** and continue installing FreeBSD.

Other Issues with FreeBSD Guest Operating Systems

- FreeBSD 4.4 installs only from CD-ROM, and not from an ISO image.

  Note: With all versions of FreeBSD there is a problem probing for the CD-ROM device `wdc1`. FreeBSD sends an illegal ATAPI command to the IDE controller and ignores the error status reply. This results in a delay of approximately one-minute each time the system boots.

- VMware does not support sound in FreeBSD guest operating systems.
- The Linux emulation support in FreeBSD 3.1 is insufficient to run the X server provided by VMware for use on Linux systems running in a virtual machine. The VGA server distributed with FreeBSD works as expected.
- The generic FreeBSD kernel works well. Users who want to configure a kernel specifically for use in a virtual machine can use a configuration file like the one below. Note that this file was created for FreeBSD 3.1.

```
#
# VMWARE -- GSX Server virtual machine
#
# For more information read the handbook part System Administration ->
# Configuring the FreeBSD Kernel -> The Configuration File.
# The handbook is available in /usr/share/doc/handbook or online as
# latest version from the FreeBSD World Wide Web server
# <URL:http://www.FreeBSD.ORG/ >
#
# An exhaustive list of options and more detailed explanations of the
# device lines is present in the ./LINT configuration file. If you are
# in doubt as to the purpose or necessity of a line, check first in LINT.
#

machine "i386"
cpu "I686_CPU"
ident VMWARE
maxusers 32

options INET #InterNETworking
options FFS #Berkeley Fast Filesystem
options FFS_ROOT #FFS usable as root device [keep this!]
options MFS #Memory Filesystem
options MFS_ROOT #MFS usable as root device, "MFS" req'ed
options NFS #Network Filesystem
options NFS_ROOT #NFS usable as root device, "NFS" req'ed
options MSDOSFS #MSDOS Filesystem
options "CD9660" #ISO 9660 Filesystem
options "CD9660_ROOT" #CD-ROM usable as root. "CD9660"req'ed
options PROCFS #Process filesystem
options "COMPAT_43" #Compatible with BSD 4.3 [KEEP THIS!]
options UCONSOLE #Allow users to grab the console
options FAILSAFE #Be conservative
options USERCONFIG #boot -c editor
options VISUAL_USERCONFIG #visual boot -c editor

config kernel root on wd0

# To make an SMP kernel, the next two are needed
#options SMP # Symmetric MultiProcessor Kernel
#options APIC_IO # Symmetric (APIC) I/O
# Optionally these may need tweaked, (defaults shown):
#options NCPU=2 # number of CPUs
#options NBUS=4 # number of busses
#options NAPIC=1 # number of IO APICs
#options NINTR=24 # number of INTs
```

```
controller isa0
controller eisa0
controller pci0

controller fdc0 at isa? port "IO_FD1" bio irq 6 drq 2
disk fd0 at fdc0 drive 0
disk fd1 at fdc0 drive 1

controller wdc0 at isa? port "IO_WD1" bio irq 14
disk wd0 at wdc0 drive 0
disk wd1 at wdc0 drive 1

controller wdc1 at isa? port "IO_WD2" bio irq 15
disk wd2 at wdc1 drive 0
disk wd3 at wdc1 drive 1

options ATAPI #Enable ATAPI support for IDE bus
options ATAPI_STATIC #Don't do it as an LKM
device acd0 #IDE CD-ROM
device wfd0 #IDE Floppy (e.g. LS-120)

device wt0 at isa? port 0x300 bio irq 5 drq 1

# atkbdc0 controls both the keyboard and the PS/2 mouse
controller atkbdc0 at isa? port IO_KBD tty
device atkbd0 at isa? tty irq 1
device psm0 at isa? tty irq 12

device vga0 at isa? port ? conflicts

# splash screen/screen saver
pseudo-device splash

# syscons is the default console driver, resembling an SCO console
device sc0 at isa? tty
# Enable this and PCVT_FREEBSD for pcvt vt220 compatible console driver
#device vt0 at isa? tty
#options XSERVER # support for X server
#options FAT_CURSOR # start with block cursor

device npx0 at isa? port IO_NPX irq 13

#
# Laptop support (see LINT for more options)
#
device apm0 at isa? disable flags 0x31 # Advanced Power Management
```

```
device sio0 at isa? port "IO_COM1" flags 0x10 tty irq 4
device sio1 at isa? port "IO_COM2" tty irq 3
device sio2 at isa? disable port "IO_COM3" tty irq 5
device sio3 at isa? disable port "IO_COM4" tty irq 9

# Parallel port
device ppc0 at isa? port? net irq 7
controller ppbus0
device nlpt0 at ppbus?
device plip0 at ppbus?
device ppi0 at ppbus?
#controller vpo0 at ppbus?

#device lnc0 at isa? port 0x1000 net irq 10 drq 0
device lnc0 # probe on PCI

pseudo-device loop
pseudo-device ether
pseudo-device sl 1
pseudo-device ppp 1
pseudo-device tun 1
pseudo-device pty 16
pseudo-device gzip # Exec gzipped a.out's

# KTRACE enables the system-call tracing facility ktrace(2).
# This adds 4 KB bloat to your kernel, and slightly increases
# the costs of each syscall.
options KTRACE #kernel tracing

# This provides support for System V shared memory and message queues.
#
options SYSVSHM
options SYSVMSG

# The `bpfilter' pseudo-device enables the Berkeley Packet Filter. Be
# aware of the legal and administrative consequences of enabling this
# option. The number of devices determines the maximum number of
# simultaneous BPF clients programs runnable.
#pseudo-device bpfilter 4 #Berkeley packet filter
```

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 113. Do not start the X server in the guest operating system until you install VMware Tools.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

11

Using Disks

Using Disks in a Virtual Machine

The following sections provide information on configuring your virtual machine's hard disk storage so it best meets your needs:

- Configuring Hard Disk Storage in a Virtual Machine on page 365
  - Disk Types: Virtual, Raw and Plain on page 365
  - Disk Modes: Persistent, Undoable and Nonpersistent on page 368
  - Additional Information about Disk, Redo-log and Lock Files on page 372
  - Defragmenting and Shrinking Virtual Disks on page 374
  - Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 376
- Adding Drives to a Virtual Machine on page 377
  - Adding New Virtual Disks to a Virtual Machine on page 377
  - Adding Existing Virtual Disks to a Virtual Machine on page 380
  - Adding Raw Disks to a Virtual Machine on page 384
  - Adding Plain Disks to a Virtual Machine on page 388
  - Adding DVD or CD-ROM Drives to a Virtual Machine on page 392
  - Adding Floppy Drives to a Virtual Machine on page 393
  - Connecting a CD-ROM or Floppy Drive to an Image File on page 394
- Installing an Operating System onto a Raw Partition from a Virtual Machine on page 396
  - Configuring a Windows Host on page 397
  - Configuring a Linux Host on page 399
- Disk Performance in Windows NT Guests on Multiprocessor Hosts on page 402

Configuring Hard Disk Storage in a Virtual Machine

Like a physical computer, a GSX Server virtual machine stores its operating system, programs and data files on one or more hard disks. Unlike a physical computer, GSX Server gives you options for undoing changes to the virtual machine's hard disk.

The New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) creates a virtual machine with one disk drive. You can use the Configuration Editor (**Settings** > **Configuration Editor**) to add more disk drives to your virtual machine, to remove disk drives from your virtual machine or to change certain settings for the existing disk drives.

The following sections describe the choices you can make in setting up hard disk storage for your virtual machine.

Disk Types: Virtual, Raw and Plain

In the most common configurations, GSX Server creates virtual hard disks, which are made up of files that are typically stored on your host computer's hard disk. In some circumstances, you may need to give your virtual machine direct access to a physical hard drive on your host computer — using the disk type known as a raw disk. Or you can choose to allocate all the space a virtual disk when you create it, which creates a type of virtual disk called a plain disk.

Virtual Disk

The disk files for a virtual disk store the information that you write to a virtual machine's hard disk — the operating system, the program files and the data files. The virtual disk files have a `.vmdk` extension.

A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. The files can be on the host machine or on a remote computer. When you configure a virtual machine with a virtual disk, you can install a new operating system onto the virtual disk without repartitioning a physical disk or rebooting the host.

IDE virtual disks can be as large as 128GB. SCSI virtual disks can be as large as 256GB. GSX Server creates a file for each 2GB of virtual disk capacity and virtual machine overhead. The actual files used by the virtual disk start out small and grow to their maximum size as needed. However, you can choose to allocate all the disk space when you create the virtual machine. This provides better performance, but you must have the disk space available on your host when you create the virtual machine.

Virtual disks can be set up as IDE disks for any guest operating system. They can be set up as SCSI disks for any guest operating system that has a driver for the BusLogic SCSI adapter used in a GSX Server virtual machine.

Note: To use SCSI disks in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP or Windows Server 2003.

A virtual disk of either type can be stored on either type of physical hard disk. That is, the files that make up an IDE virtual disk can be stored on either an IDE hard disk or a SCSI hard disk. So can the files that make up a SCSI virtual disk. They can also be backed up on other types of fast-access storage media, such as DVD-ROM or CD-ROM discs. For information about running virtual machines from DVD-ROM or CD-ROM, see Running Virtual Machines from DVD-ROM or CD-ROM Discs on page 235.

A key advantage of virtual disks is their portability. Because the virtual disks are stored as files on the host machine or a remote computer, you can move them to a new location on the same computer or to a different computer. You can also use GSX Server on a Windows host to create virtual disks, then move them to a Linux computer and use them under GSX Server for Linux — or vice versa. For information about moving virtual disks, see Moving and Sharing Virtual Machines on page 242.

Note: Beginning with GSX Server 2, virtual disks are created in a new format that is not recognized by earlier VMware products except for VMware Workstation 3.0 and later. Future versions of other VMware products will support this new virtual disk format. GSX Server 2 supports virtual disks created in the old format; to convert these disks to the new format, shrink the virtual disks. For more information, see Defragmenting and Shrinking Virtual Disks on page 374.

Raw Disk

A raw disk directly accesses an existing local disk or partition. You can use raw disks if you want GSX Server to run one or more guest operating systems from existing disk partitions. Raw disks may be set up on both IDE and SCSI devices. At this time, however, booting from an operating system already set up on an existing SCSI disk or partition is not supported.

The most common use of a raw disk is for converting a dual-boot or multiple-boot machine so one or more of the existing operating systems can be run inside a virtual machine.

Caution: If you run an operating system natively on the host computer, the switch to running it inside a virtual machine is like pulling the hard drive out of one computer

and installing it in a second computer with a different motherboard and other hardware. You need to prepare carefully for such a switch. The specific steps you need to take depend on the operating system you want to use inside the virtual machine.

You can also create a new virtual machine using a raw disk. For details, see Installing an Operating System onto a Raw Partition from a Virtual Machine on page 396. In most cases, however, it is better to use a virtual disk.

Only expert users should attempt raw disk configurations.

Plain Disk

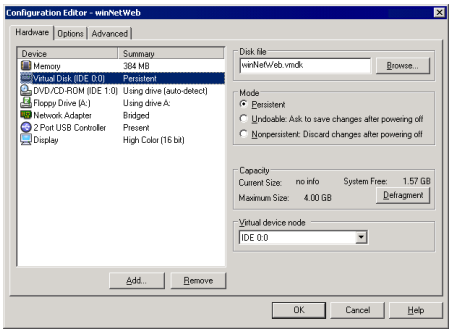
A plain disk is a type of virtual disk that provides another way to create large disks for the virtual machine. The difference is that, for a plain disk, the full capacity of the disk is allocated when you create the disk, provided the space is available on the host. Plain disks can be as large as 128GB.

Virtual disks with their disk space pre-allocated perform better and you can install the guest operating system faster. A plain disk is useful for clustering virtual machines. For more information about clustering, see High-Availability Configurations with GSX Server on page 539.

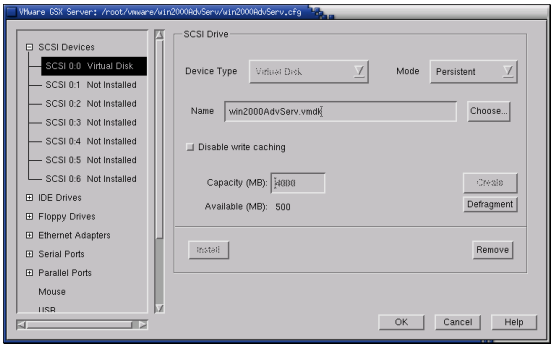
Virtual machines with plain disks created in GSX Server 1 run under GSX Server 2.

Disk Modes: Persistent, Undoable and Nonpersistent

You can use the Configuration Editor (**Settings** > **Configuration Editor**) to configure disks in one of three modes: persistent, undoable and nonpersistent.



The Configuration Editor on a Windows host shows an IDE virtual disk configured as undoable



The Configuration Editor on a Linux host shows installation of a SCSI virtual disk configured as persistent

Disk modes determine how changes are saved to the disk. Raw, virtual and plain disks can use any available mode. For example, a user could have an undoable raw disk, an undoable virtual disk or an undoable plain disk.

Persistent

Disks in persistent mode are the simplest to use. Disks in persistent mode behave like conventional disk drives on your physical computer. All data written to a disk in persistent mode are written out permanently to the disk. The behavior is the same for all disk types.

Undoable

When you power off a virtual machine with a disk in undoable mode, any changes to the disk can be committed, saved until the virtual machine is powered on again or discarded.

This is especially useful for experimenting with new configurations or unfamiliar software. Because of the disaster-recovery possibilities this mode offers, many users prefer to set disks in undoable mode as a standard part of their configurations.

When data is written to an undoable mode disk, the changes are stored in a file called a redo log. A disk in undoable mode gives you the option later of permanently applying the changes saved in the redo log, so they become part of the main disk files.

While the virtual machine is running, disk blocks that have been modified and written to the redo log are read from there instead of from the disk files.

Any disk type can be used in undoable mode.

When you power off a virtual machine with a disk in undoable mode, you are given three options:

- Commit the changes in the redo log to the disk
- Discard the changes in the redo log
- Keep the redo log

If you choose to commit the redo log, the changes in the redo log are applied to the disk. The redo-log file is deleted.

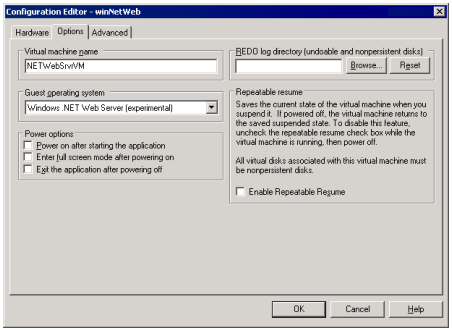
If you choose to discard the redo log, any changes in the redo log are **not** applied to the disk. The disk returns to the state it was in before changes began accruing in the redo log.

If you choose to keep the redo log, the next time you power on the virtual machine GSX Server detects the redo-log file and prompts you to either commit the redo log changes made from the last time the virtual machine ran, discard the redo log, continue appending changes to the redo log or cancel the power on.

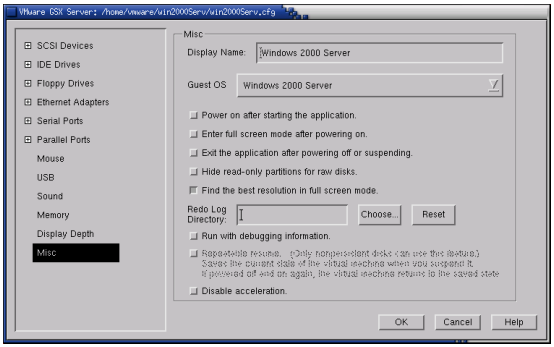
The amount of space required by a redo log varies with the amount of information that has changed in the guest operating system and the frequency with which you commit changes. The longer the time between commitments of the redo log, the larger it grows.

The redo-log file is placed in the same folder (directory) as the disk file by default. However, you can change the location of the redo-log file in the Configuration Editor.

On a Windows host, click the **Options** tab, then type in or browse to the folder in which the redo log should be stored.


Configuration Editor - winNetWeb
Hardware
Options
Advanced
Virtual machine name
NETWebSrvVM
REDO log directory (undoable and nonpersistent disks)
Browse...
Reset
Guest operating system
Windows .NET Web Server (experimental)
Repeatable resume
Saves the current state of the virtual machine when you suspend it. If powered off, the virtual machine returns to the saved suspended state. To disable this feature, uncheck the repeatable resume check box while the virtual machine is running, then power off.
Power options
Power on after starting the application
Enter full screen mode after powering on
Exit the application after powering off
All virtual disks associated with this virtual machine must be nonpersistent disks.
Enable Repeatable Rejume
OK
Cancel
Help

On a Linux host, click **Misc** on the left side of the Configuration Editor, then type in or choose the directory in which the redo log should be stored.



Nonpersistent

Changes to disks in nonpersistent mode are not saved to the disks, but are lost when the virtual machine is powered off or reset.

Nonpersistent mode is convenient for people who always want to start with a virtual machine in the same state. Example uses include providing known environments for software test and technical support users as well as doing demonstrations of software.

Any disk type can be used in nonpersistent mode.

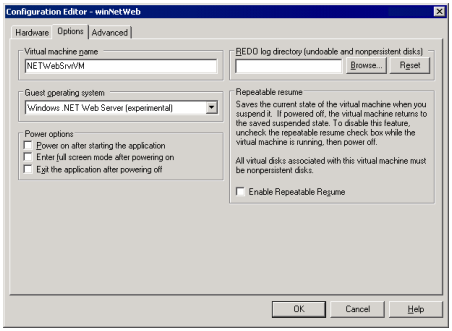
If your virtual disks are in nonpersistent mode, you can take advantage of the repeatable resume feature, which allows you to save the current state of the virtual machine when you suspend it, then resume from the point at which you suspended it

every time you start the virtual machine. For more information, see Resuming Virtual Machines Repeatedly from the Same Point on page 231.

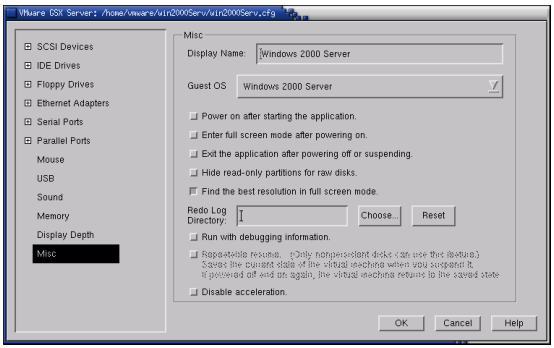
GSX Server only reads the virtual disk file. Any writes to the virtual disk are actually written to a redo-log file. While you are running the virtual machine, any blocks that have been modified and written to the redo-log file are read from the redo-log file instead of the disk files. The redo-log file is deleted when you power off or reset the virtual machine. This is similar to the redo-log files used with disks in undoable mode.

The redo-log file is placed by default in the folder defined by the host operating system's temp directory. However, the location of the redo-log file can be changed in the Configuration Editor.

On a Windows host, click the **Options** tab, then type in or browse to the folder in which the redo log should be stored.


Configuration Editor - winNetWeb
Hardware
Options
Advanced
Virtual machine name
NETWebSrvVM
REDO log directory (undoable and nonpersistent disks)
Browse...
Reset
Guest operating system
Windows .NET Web Server (experimental)
Repeatable resume
Saves the current state of the virtual machine when you suspend it. If powered off, the virtual machine returns to the saved suspended state. To disable this feature, uncheck the repeatable resume check box while the virtual machine is running, then power off.
All virtual disks associated with this virtual machine must be nonpersistent disks.
Power options
Power on after starting the application
Enter full screen mode after powering on
Exit the application after powering off
Enable Repeatable Resume
OK
Cancel
Help

On a Linux host, click **Misc** on the left side of the Configuration Editor, then type in or choose the directory in which the redo log should be stored.



Additional Information about Disk, Redo-log and Lock Files

Disk Files

When you are creating a new virtual machine, you can choose to use an existing virtual disk (on a Windows host, you must select the custom path when creating the virtual machine).

The Configuration Editor (**Settings** > **Configuration Editor**) allows you to choose different disk files for a virtual machine. You may need to do this if you moved the disk files to a new location.

The disk files for a virtual disk store the information that you write to a virtual machine's hard disk — the operating system, the program files and the data files. The virtual disk files have a `.vmdk` extension.

A virtual disk comprises one or more `.vmdk` files. The larger the size of the virtual disk, the more `.vmdk` files. As data is added to a virtual disk, the `.vmdk` files grow in size, to a maximum of 2GB each. Almost all of a `.vmdk` file's content is the virtual machine's data, with a small portion allotted to virtual machine overhead.

If the virtual disk needs 2GB or more disk space, the Configuration Editor shows the name of the first file in the set of files used to store the virtual disk. The other files used for that disk are automatically given names based on the first file's name. For example, a Windows 2000 virtual machine that needed two files to store its virtual disk would, by default, store it in files named `Windows 2000.vmdk` and `Windows 2000-02.vmdk`.

Note: If you choose to allocate the space for a virtual disk when you create it, the virtual disk files have a special format. The file that stores information about the virtual disk has a `.pln` extension and the files used to store the virtual disk's data have a `.dat` extension.

If your virtual machine is on a Windows host and uses disk files created under earlier VMware products, with a `.dsk` extension, they can be updated to use the new extension. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 376.

If you are using a raw disk, a file with the extension `.raw` stores information about the physical disk or partition used by the virtual machine.

Redo-Log Files

Redo-log files save blocks that the virtual machine modifies while it is running. The redo-log file for a disk in nonpersistent mode is not saved when the virtual machine is powered off or reset, while the redo-log file for a disk in undoable mode is saved. The

redo-log file for disks in undoable mode is called the redo log, and the user decides whether the redo-log file should be saved or not.

The redo-log file for a virtual disk called `vm` is called `vm.vmdk.REDO`. If the virtual disk is larger than 2GB, it is divided into sets of 2GB disk files named `vm.vmdk`, `vm-02.vmdk`, `vm-03.vmdk` and so on; its redo-log files are called `vm.vmdk.REDO`, `vm-02.vmdk.REDO`, `vm-03.vmdk.REDO` and so on.

You can choose the location where these redo logs are stored. By default, the redo logs for disks in undoable mode are stored in the same directory as the virtual disk (`.vmdk`) file. Redo logs for disks in nonpersistent mode are stored in your host's temp directory by default. In the case of plain disks, `filename.pln.REDO` is created by default in the same directory as the `.pln` file.

By default, redo-log files for raw disks are located in the same directory as the virtual machine configuration file.

You can change the location of the log file for disks in nonpersistent and undoable modes in the Configuration Editor.

On a Windows host, click the **Options** tab, then type in or browse to the folder in which the redo log should be stored.

On a Linux host, click **Misc** on the left side of the Configuration Editor, then type in or choose the directory in which the redo log should be stored.

You may choose to locate the redo-log files in a different directory to increase available space or improve performance. For best performance, the log files for a virtual machine should be on a local hard drive on the host computer.

Lock Files

A running virtual machine creates lock files to prevent consistency problems on virtual disks. If the virtual machine did not use locks, multiple virtual machines might read and write to the disk, causing users to lose data.

Lock files are always created in the same folder (directory) as the `.vmdk` or `.pln` file. There are two types of lock files — reader and writer. A disk in nonpersistent mode is protected by reader lock files, while disks in persistent and undoable modes use writer lock files.

A disk protected by a writer lock file can be accessed by only one virtual machine.

A disk that has reader lock files can be read by more than one virtual machine but cannot be written to.

The data storage files of a plain disk are individually locked, using the same method.

Note: The locking methods used by GSX Server on Windows and Linux hosts are different, so files shared between them are not fully protected. If you use a common file repository that provides files to users on both Windows and Linux hosts, be sure that each virtual machine is run by only one user at a time.

When a virtual machine is powered off, it removes lock files it created. If it cannot remove the lock, a stale lock file is left protecting the `.vmdk` or `.pln` file. For example, if the host machine crashes before the virtual machine has a chance to remove its lock file, there is a stale lock.

If a stale lock file remains when the virtual machine is started again, the virtual machine tries to remove the stale lock. To make sure that no virtual machine could be using the lock file, the virtual machine checks the lock file to see if:

1. The lock was created on the same host where the virtual machine is running.
2. The process that created the lock is not running.

If those two conditions are true, the virtual machine can safely remove the stale lock. If either of those conditions is not true, a dialog box appears explaining what you can do about the lock.

Raw disk partitions are also protected by locks. However, the host operating system is not aware of this locking convention and thus does not respect it. For this reason, VMware strongly recommends that the raw disk for a virtual machine not be installed on the same physical disk as the host operating system.

Defragmenting and Shrinking Virtual Disks

Defragmenting Virtual Disks

Defragmenting disks rearranges files, programs and unused space on the virtual disk so that programs run faster and files open more quickly. Defragmenting does not reclaim unused space on a virtual disk; to reclaim unused space, shrink the disk.

For best disk performance, you can take the following three actions, in the order listed:

1. Run a disk defragmentation utility inside the virtual machine.
2. When the virtual machine is powered off, defragment its virtual disks from the Configuration Editor (**Settings** > **Configuration Editor**). Select the virtual disk you want to defragment, then click **Defragment**.

   Note: This capability only works with virtual disks, not raw or plain disks.
3. Run a disk defragmentation utility on the host computer.

Defragmenting disks may take considerable time.

Shrinking Virtual Disks

Shrinking a virtual disk reclaims unused space in the virtual disk. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. You cannot shrink raw or plain disks.

Shrinking virtual disks is a convenient way to convert a virtual disk to the new format supported by GSX Server 2. Virtual disks created in the new format cannot be recognized by earlier VMware products except for VMware Workstation 3.0 and later.

The virtual disks to be shrunk must be booted in persistent mode. You can change the mode of a virtual disk before the virtual machine is powered on. See Disk Modes: Persistent, Undoable and Nonpersistent on page 368. Shrinking requires free disk space on the host equal to the size of the virtual disk being shrunk.

Shrinking a disk is a two-step process: the first step, called wiping, is where VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. This allows for the maximum shrink possible. Wiping takes place in the guest operating system.

The shrink process itself is the second step, and it takes place outside the virtual machine. GSX Server reduces the size of the disk based on the disk space reclaimed by the wipe process. This step occurs after the wipe finishes preparing the disk for shrinking.

When a virtual machine is powered on, you can shrink its virtual disks from the VMware Tools control panel.

In a Linux guest operating system, to prepare virtual disks for shrinking, you should run VMware Tools as the root user. This way, you ensure the whole virtual disk is shrunk. Otherwise, if you shrink disks as a non-root user you cannot wipe the parts of the virtual disk that require root-level permissions.

1. To launch the control panel in a Windows guest, double-click the VMware Tools icon in the system tray or choose **Start** > **Settings** > **Control Panel**, then double-click VMware Tools.

   To launch the control panel in a Linux guest, become root (`su -`, if you want to shrink parts of the disk restricted to root access), then run `vmware-toolbox &`
2. Click the **Shrink** tab.
3. Select the virtual disks you want to wipe, then click **Prepare to Shrink**.

Note: If you deselect some of the partitions to wipe, the whole disk is still shrunk. However, those partitions are not prepared for shrinking, and the shrink does not reduce the size of the virtual disk as much as it could otherwise.

4. When VMware Tools finishes wiping the selected disk partitions, you are prompted to begin shrinking the disks.

Shrinking disks may take considerable time.

Updating Filenames for Virtual Disks Created with Earlier VMware Products

Except for VMware Workstation 3.0 and later, previous VMware products, including GSX Server 1, named virtual disk files with a `.dsk` extension. GSX Server now uses a `.vmdk` extension for those files. During installation of the GSX Server 2 software on a Windows host, GSX Server offers to update existing virtual disk files automatically. It also automatically updates references to the virtual disk files in the configuration files for the virtual machine.

In addition, GSX Server converts the filename extensions for the files that store the state of a suspended virtual machine. The old extension was `.std`. The new extension is `.vmss`.

This feature only exists on Windows hosts. It is not necessary to rename the files on a Linux host. However, if you move the virtual machine to a Windows host, you can rename the files at that time.

Running the Updater at a Later Time

On a Windows host computer, you can run the filename updater at any time. To do so, follow these steps.

1. Open a command prompt.
2. Change to the folder in which the GSX Server program files are installed. If you installed the files in the default locations, use this command.

   ```
   cd C:\Program Files\VMware\VMware GSX Server
   ```

3. Run the updater.

   ```
   dskrename.exe
   ```

Adding Drives to a Virtual Machine

GSX Server virtual machines can use up to four IDE devices and up to seven SCSI devices. Any of these devices can be a virtual hard disk or DVD or CD-ROM drive. A virtual machine can read data from a DVD-ROM disc. GSX Server does not support playing DVD movies in a virtual machine.

Many other SCSI devices can be connected to a virtual machine using the host operating system's generic SCSI driver. For details on connecting these devices, see Connecting to a Generic SCSI Device on page 517.

The following sections describe how to add virtual disks, raw disks, DVD-ROM/CD-ROM drives and floppy drives to virtual machines. In addition, you can connect CD-ROM and floppy drives to disk image files.

Adding New Virtual Disks to a Virtual Machine

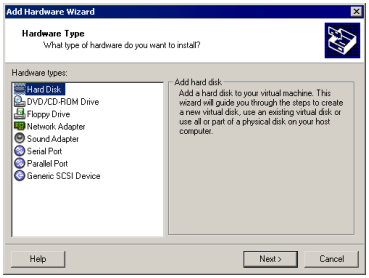
Virtual disks are stored as files on the host computer or on a network file server, so it does not matter whether the disk that holds the files is IDE or SCSI. A virtual IDE drive can be stored on an IDE drive or on a SCSI drive. So can a virtual SCSI drive.

Windows Host

Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a new virtual disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the console toolbar.

Note: If you have a Windows NT 4.0 guest with a SCSI virtual disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and click **Add**. The Add Hardware Wizard guides you through the steps to create your virtual disk.


Add Hardware Wizard
Hardware Type
What type of hardware do you want to install?
Hardware types:
Hard Disk
DVD/CD-ROM Drive
Floppy Drive
Network Adapter
Sound Adapter
Serial Port
Parallel Port
Generic SCSI Device
Add hard disk
Add a hard disk to your virtual machine. This wizard will guide you through the steps to create a new virtual disk, use an existing virtual disk or use all or part of a physical disk on your host computer.
Help
Next >
Cancel

2. Click **Hard Disk**, then click **Next**.
3. Select **Create a New Virtual Disk**, then click **Next**.
4. Set the size for the new virtual disk.

   Note: The virtual disk's files start small and grow as needed, but they can never grow larger than the size you set here. You can set a size between 2GB and 256GB for a SCSI virtual disk or 128GB for an IDE virtual disk. The default is 4GB.
5. Accept the default filename and location for the virtual disk file or change it. To use a different name or location, click **Browse**.

   In most cases, the wizard creates a SCSI virtual disk by default. If your guest operating system does not have appropriate support for the virtual SCSI adapter in the virtual machine, the wizard creates an IDE virtual disk. If you want your virtual disk to be an IDE device, click **Advanced** and be sure the virtual device node is set to an available IDE node.

   When you have set the filename and location you want to use and made any selections you want to make on the Select a Device Node screen, click **Finish**.

   Note: To use SCSI disks in a Windows Server 2003 or Windows XP virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows Server 2003 or Windows XP.
6. The wizard creates the new virtual disk. It appears to your guest operating system as a new, blank hard disk. Use the guest operating system's tools to partition and format the new drive for use.

   The new virtual disk is set up in persistent mode. To change to nonpersistent or undoable mode, use the Configuration Editor. Click the entry for the new virtual disk, then select the mode you want.

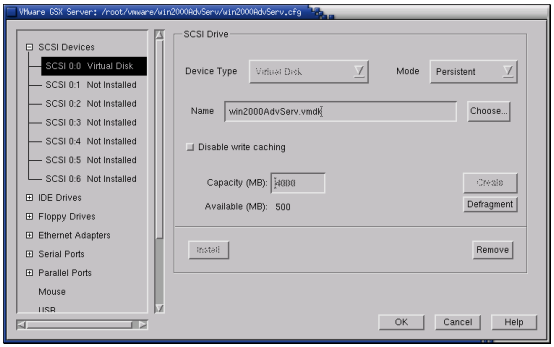
   If the virtual disk files are stored on a network file server, you can improve performance of the virtual disk in undoable mode by setting its redo log to a location on the host computer. You can make this setting on the **Options** tab of the Configuration Editor.

Linux Host

Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a new virtual disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the console toolbar.

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). If you want to add a SCSI virtual disk, click the + sign beside **SCSI Devices**. If you want to add an IDE virtual disk, click the + sign beside **IDE Drives**.

   Note: All virtual machines can use IDE virtual disks. SCSI virtual disks can be used with guest operating systems that have drivers for the virtual BusLogic SCSI adapter used in the virtual machine. To use SCSI disks in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP or Windows Server 2003.



2. Click a device that is shown as **Not Installed**.
3. Use the default device type of **Virtual Disk**.
4. Keep the default mode of **Persistent** or use the drop-down list to change the setting to **Undoable** or **Nonpersistent**.
5. Type the name for the virtual disk's first file. By default, it is created in the same directory as the virtual machine's configuration file. To create it in a different directory, type the full path name or click **Choose** to navigate to the directory you want to use.
6. Set the capacity for the new virtual disk.

Note: The virtual disk's files start small and grow as needed, but they can never grow larger than the size you set here. You can set a size between 2000 (2GB) and 256000MB (256GB) for a SCSI virtual disk or 128000 (128GB) for an IDE virtual disk. The default is 4000 (4GB).

7. If you are connecting to a virtual machine on a Linux host and you want to disable write caching on this disk, select **Disable write caching**.

   When write caching is enabled, there is a delay between the time a program saves data and the time that data is actually written to disk. This improves performance. But the delay in writing data to disk adds some risk of data loss. Thus if data integrity is more important than performance, you may want to disable write caching.

8. Click **Create** to create the files for your new virtual disk.
9. Click **Install** to install the new virtual disk in your virtual machine.
10. Click **OK** to save the configuration and close the Configuration Editor.

    The new virtual disk appears to your guest operating system as a new, blank hard disk. Use the guest operating system's tools to partition and format the new drive for use.

    If the virtual disk files are stored on a network file server, you can improve performance of the virtual disk by setting the redo log directory to a location on the host computer. You can make this setting in the **Misc** panel of the Configuration Editor.

Adding Existing Virtual Disks to a Virtual Machine

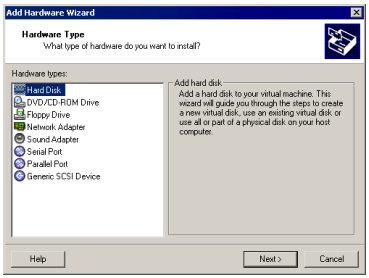
Virtual disks are stored as files on the host computer or on a network file server, so it does not matter whether the disk that holds the files is IDE or SCSI. A virtual IDE drive can be stored on an IDE drive or on a SCSI drive. So can a virtual SCSI drive.

Use the Configuration Editor (**Settings** > **Configuration Editor**) to add an existing virtual disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the console toolbar.

Windows Host

Note: If you have a Windows NT 4.0 guest with a SCSI virtual disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

1. With the virtual machine powered off, open the Configuration Editor (**Settings** > **Configuration Editor**) and click **Add**. The Add Hardware Wizard guides you through the steps to create your virtual disk.


Add Hardware Wizard
Hardware Type
What type of hardware do you want to install?
Hardware types:
Hard Disk
DVD/CD-ROM Drive
Floppy Drive
Network Adapter
Sound Adapter
Serial Port
Parallel Port
Generic SCSI Device
Add hard disk
Add a hard disk to your virtual machine. This wizard will guide you through the steps to create a new virtual disk, use an existing virtual disk or use all or part of a physical disk on your host computer.
Help
Next >
Cancel

2. Click **Hard Disk**, then click **Next**.
3. Select **Use an Existing Virtual Disk**, then click **Next**.
4. In the **Existing disk file** field, type the path to the virtual disk, or click **Browse** and navigate to the directory containing the disk you want to use. Click **Next**.
5. Choose the disk mode. Select **Persistent**, **Undoable** or **Nonpersistent**, then click **Next**.
6. If you selected a SCSI disk, click **Advanced** and be sure the virtual device node is set to an available SCSI node.

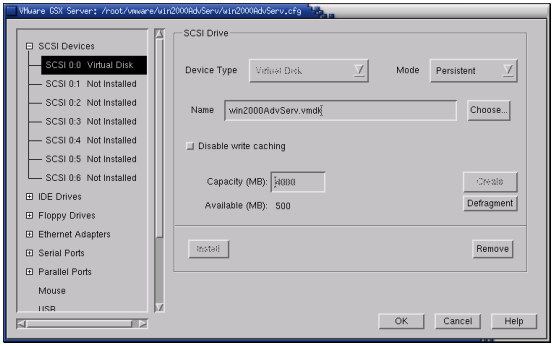
   Note: To use SCSI disks in a Windows Server 2003 or Windows XP virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows Server 2003 or Windows XP.
7. When you have set the filename and location you want to use and made any selections you want to make on the Select a Device Node screen, click **Finish**.

   If the virtual disk files are stored on a network file server, you can improve performance of the virtual disk in undoable mode by setting its redo log to a location on the host computer. You can make this setting on the **Options** tab of the Configuration Editor.

Linux Host

1. With the virtual machine powered off, open the Configuration Editor (**Settings** > **Configuration Editor**). If you want to add a SCSI virtual disk, click the + sign beside **SCSI Devices**. If you want to add an IDE virtual disk, click the + sign beside **IDE Drives**.

   Note: All virtual machines can use IDE virtual disks. SCSI virtual disks can be used with guest operating systems that have drivers for the virtual BusLogic SCSI adapter used in the virtual machine. To use SCSI disks in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP or Windows Server 2003.



2. Click a device that is shown as **Not Installed**.
3. Use the default device type of **Virtual Disk**.
4. Keep the default mode of **Persistent** or use the drop-down list to change the setting to **Undoable** or **Nonpersistent**.
5. Click **Choose** to navigate to the directory containing the disk you want to use.
6. If you want to disable write caching on this disk, select **Disable write caching**.

   When write caching is enabled, there is a delay between the time a program saves data and the time that data is actually written to disk. This improves performance. But the delay in writing data to disk adds some risk of data loss. Thus if data integrity is more important than performance, you may want to disable write caching.
7. Click **Install** to add the virtual disk to your virtual machine.

8. Click **OK** to save the configuration and close the Configuration Editor.

   If the virtual disk files are stored on a network file server, you can improve performance of the virtual disk by setting the redo log directory to a location on the host computer. You can make this setting in the **Misc** panel of the Configuration Editor.

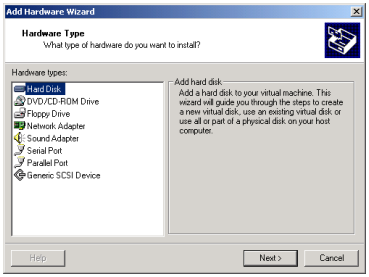
Adding Raw Disks to a Virtual Machine

Windows Host

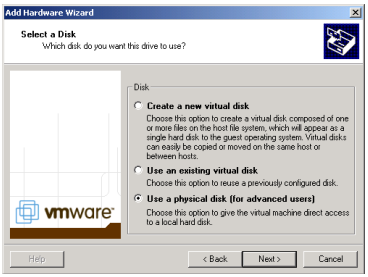
Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a new raw disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the console toolbar.

Caution: Raw disks are an advanced feature and should be configured only by expert users.

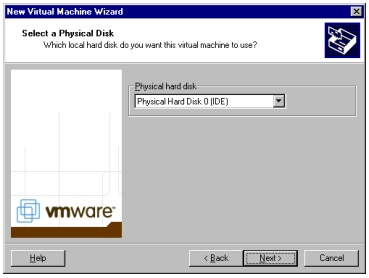
1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and click **Add**. The Add Hardware Wizard guides you through the steps to create your virtual disk.
2. Click **Hard Disk**, then click **Next**.


Add Hardware Wizard
Hardware Type
What type of hardware do you want to install?
Hardware types:
Hard Disk
DVD/CD-ROM Drive
Floppy Drive
Network Adapter
Sound Adapter
Serial Port
Parallel Port
Generic SCSI Device
Add hard disk
Add a hard disk to your virtual machine. This wizard will guide you through the steps to create a new virtual disk, use an existing virtual disk or use all or part of a physical disk on your host computer.
Help
Next >
Cancel

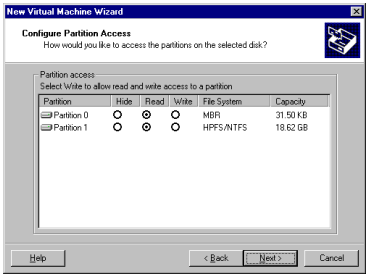
3. Select **Use a physical disk**, then click **Next**.


Add Hardware Wizard
Select a Disk
Which disk do you want this drive to use?
Disk
Create a new virtual disk
Choose this option to create a virtual disk composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk.
vmware
Help
< Back
Next >
Cancel

4. Choose the physical hard disk to use from the drop-down list. Click **Next**.



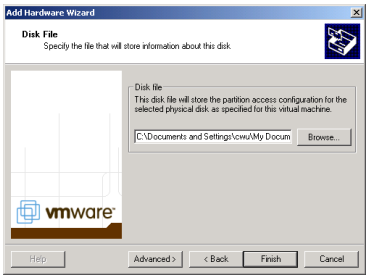
5. Set the virtual machine's access rights for each partition on the physical hard disk.



- Select **Hide** if the virtual machine should not see the partition.
- Select **Read** to give the virtual machine read-only access to the partition.
- Select **Write** to give the virtual machine read/write access to the partition.

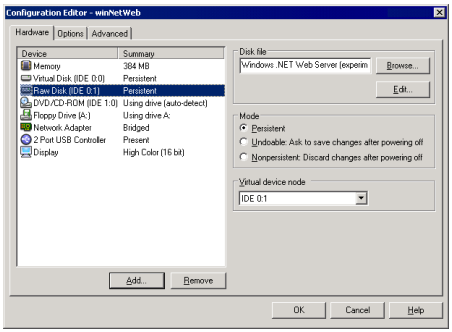
6. Click **Next**.

7. Accept the default filename and location for the file that stores access information for this raw disk — or change it, if you want to use a different name or location. To find a different directory, click **Browse**.



When you have set the filename and location you want to use and made any selections you want to make on the advanced settings screen, click **Finish**.

8. The wizard configures the new raw disk. If the partitions used on the raw disk are not formatted for your guest operating system, use the guest operating system's tools to format them.



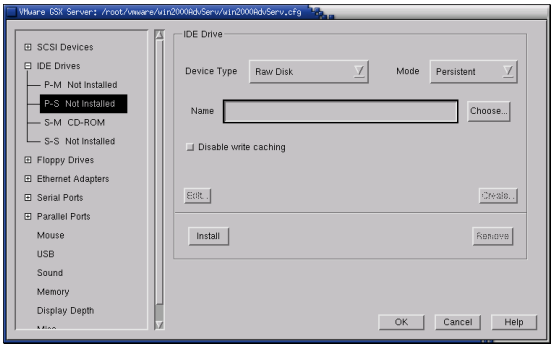
The new raw disk is set up in persistent mode. To change to nonpersistent or undoable mode, use the Configuration Editor. Click the entry for the new raw disk, then select the mode you want.

Linux Host

Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a new raw disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the console toolbar.

Caution: Raw disks are an advanced feature and should be configured only by expert users.

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). If you want to add a SCSI raw disk, click the + sign beside **SCSI Devices**. If you want to add an IDE raw disk, click the + sign beside **IDE Drives**.



2. Click a device that is shown as **Not Installed**.
3. Choose **Raw Disk** from the **Device Type** drop-down list.
4. Keep the default mode of **Persistent** or use the drop-down list to change the setting to **Undoable** or **Nonpersistent**.
5. Type the name for the file that will store access information for this raw disk. To create it in a different directory, type the full path name or click **Choose** to navigate to the directory you want to use.
6. If you are connecting to a virtual machine on a Linux host and you want to disable write caching on this disk, select **Disable write caching**.

   When write caching is enabled, there is a delay between the time a program saves data and the time that data is actually written to disk. This improves performance. But the delay in writing data to disk adds some risk of data loss. Thus if data integrity is more important than performance, you may want to disable write caching.
7. Click **Create** to create the file for your new raw disk.
8. A dialog box prompts you for the name of the device that holds the partition you want to use as a raw disk. Enter the path to the device — for example `/dev/hdb` — then click **OK**.

9. A dialog box prompts you to set access permissions for the partitions on the device you have selected.
   - Select **No Access** if the virtual machine should not see the partition.
   - Select **Read Only** to give the virtual machine read-only access to the partition.
   - Select **Read/Write** to give the virtual machine read/write access to the partition.

   Click **Save** to save your selections and close the dialog box.
10. Click **Install** to install the new raw disk in your virtual machine.
11. Click **OK** to save the configuration and close the Configuration Editor.
12. If the partitions used on the raw disk are not formatted for your guest operating system, use the guest operating system's tools to format them.

Adding Plain Disks to a Virtual Machine

Plain disks are a type of virtual disk that provides faster virtual machine performance. Since you allocate all the disk space when you create the plain disk, the plain disk runs faster in a virtual machine than a virtual disk. Also, the time it takes to install the guest operating system is reduced. The drawback is that you need to have all the space you want to allocate to the plain disk available when you create the disk. Also, plain disks take longer to create; the larger the disk, the longer it takes to create.

Another area in which they have a place is SCSI reservation (and high-availability configurations). VMware supports SCSI reservation when used with plain disks; support for SCSI reservation with virtual and raw disks is considered experimental. For more information about SCSI reservation, see High-Availability Configurations with GSX Server on page 539.

Any plain disks you created in GSX Server 1 can run in virtual machines created under GSX Server 2 and can be shared through SCSI reservation.

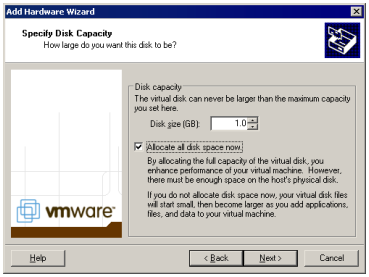
To create a plain disk, follow the steps below for your host operating system. You need to specify the size of the plain disk, up to 128GB. Remember that, unlike virtual disks, which grow as data is added to them, all the space the plain disk is to occupy on the host is allocated when the disk is created.

A plain disk is composed of at least 2 files, a `.pln` file and one or more `.dat` files. The `.pln` file is a text file that maps the `.dat` files to the corresponding sectors of the plain disk. The `.dat` file or files contain the data for the disk. Each `.dat` file is limited to 2GB in size. If the plain disk (named, for example, `plaindisk.pln`) is larger than 2GB, then its `.dat` files are divided into sets of 2GB data files named `plaindisk1.dat`, `plaindisk2.dat`, `plaindisk3.dat` and so on.

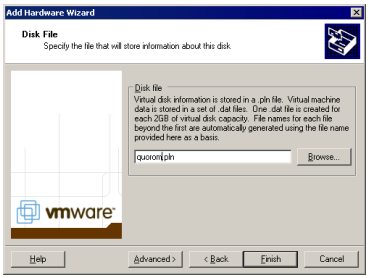
Windows Host

To create a plain disk on a Windows host, you use the Add New Hardware Wizard in the Configuration Editor. When you are creating the new virtual disk, you must make one specific selection. Follow the steps below.

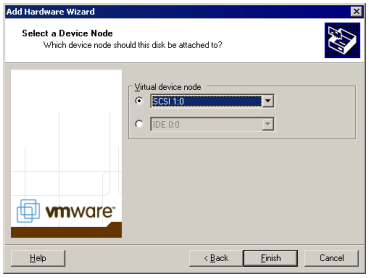
1. Connect to the virtual machine with a console then choose **Settings** > **Configuration Editor** to open the Configuration Editor. Do not power on the virtual machine.
2. Click **Add** to begin adding a plain disk. The Add Hardware Wizard opens.
3. Choose a Hardware Type of **Hard Disk** then click **Next**.
4. Select **Create a new virtual disk** and click **Next**.
5. Specify the size of the disk, check **Allocate all disk space now** then click **Next**.


Add Hardware Wizard
Specify Disk Capacity
How large do you want this disk to be?
Disk capacity
The virtual disk can never be larger than the maximum capacity you set here.
Disk size (GB):
1.0
Allocate all disk space now.
By allocating the full capacity of the virtual disk, you enhance performance of your virtual machine. However, there must be enough space on the host's physical disk.
If you do not allocate disk space now, your virtual disk files will start small, then become larger as you add applications, files, and data to your virtual machine.
vmware
Help
< Back
Next >
Cancel

6. If you prefer, change the name of the plain disk.


Add Hardware Wizard
Disk File
Specify the file that will store information about this disk
Disk file
Virtual disk information is stored in a .pln file. Virtual machine data is stored in a set of .dat files. One .dat file is created for each 2GB of virtual disk capacity. File names for each file beyond the first are automatically generated using the file name provided here as a basis.
quorom.pln
Browse...
vmware
Help
Advanced >
< Back
Finish
Cancel

7. If you want to set the disk to run on a specific node, click **Advanced**.

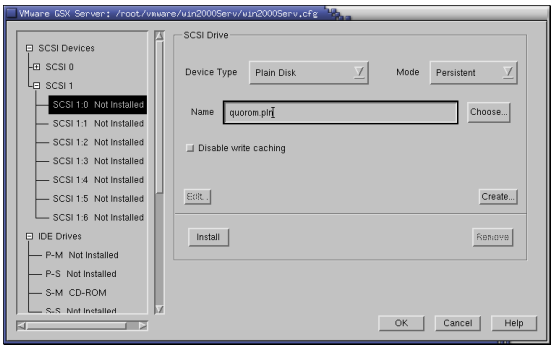


8. Specify the node, then click **Finish**.
9. Power on the virtual machine and format the plain disk.

Linux Host

To create a plain disk on a Linux host, use the Configuration Editor (**Settings** > **Configuration Editor**). The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the GSX Server console toolbar.

1. Connect to the virtual machine with a console then choose **Settings** > **Configuration Editor** to open the Configuration Editor. Do not power on the virtual machine.
2. To add a SCSI plain disk, click the **+** sign beside **SCSI Devices**. Click a device on a SCSI controller that is shown as **Not Installed**.



3. Select the device type of **Plain Disk**.

4. Keep the default mode of **Persistent** or use the drop-down list to change the setting to **Undoable** or **Nonpersistent**.
5. Type the name for the plain disk's first file. By default, it is created in the same directory as the virtual machine's configuration file. To create it in a different directory, type the full path name or click **Choose…** to navigate to the directory you want to use.
6. Set the capacity for the new plain disk. The capacity cannot be greater than 128,000MB (128GB).

   Note: Unlike a virtual disk, which starts small and grows as data is added to it, when the plain disk is created, all the space is allocated to it up front. Be sure you have enough room on the host to hold the plain disk you are creating.
7. If you are connecting to a virtual machine on a Linux host and you want to disable write caching on this disk, click the check box beside **Disable Write Caching**.

   When write caching is enabled, there is a delay between the time a program saves data and the time that data is actually written to disk. This improves performance. But the delay in writing data to disk adds some risk of data loss. Thus if data integrity is more important than performance, you may want to disable write caching.
8. Click **Create** to create the files for your new plain disk.
9. Click **OK** to save your settings and close the Configuration Editor.

   The new plain disk appears to your guest operating system as a new, blank hard disk. Use the guest operating system's tools to partition and format the new drive for use. If you are sharing this disk for clustering, install and set up clustering software on the plain disk.

Adding DVD or CD-ROM Drives to a Virtual Machine

You can add one or more DVD or CD-ROM drives to your virtual machine. You can connect the virtual machine's drive to a physical drive on the host machine or to an ISO image file.

You can configure the virtual DVD or CD-ROM drive as either IDE or SCSI, no matter what kind of physical drive to which you connect it. In other words, if your host computer has an IDE CD-ROM drive, you can set up the virtual machine's drive as either SCSI or IDE and connect it to the host's drive. The same is true if the host's physical drive is a SCSI drive.

The DVD or CD-ROM drives in the virtual machine can be used to read data from CD-ROM or DVD-ROM disks. GSX Server does not support playing DVD movies in a virtual machine.

If you need to read from multisession discs, configure your DVD/CD-ROM drive to use raw access mode.

Adding a DVD or CD-ROM Drive on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and click **Add** to start the Add Hardware Wizard.
2. Click **DVD/CD-ROM Drive**, then click **Next**.
3. Select **Use physical drive** if you want to connect the virtual machine's drive to a physical drive on the host computer. Select **Use ISO Image** if you want to connect the virtual machine's drive to an ISO image file.
4. Do one of the following:
   - If you selected **Use physical drive**, choose the drive you want to use from the drop-down list, then click **Finish**.
   - If you selected **Use ISO Image**, enter the path and filename for the image file or click **Browse** to navigate to the file. Then click **Finish**.
5. The drive is set up initially so it appears to the guest operating system as an IDE drive. If you want to change so it appears to the guest operating system as a SCSI drive, click the drive's entry in the Configuration Editor and make that change in the settings panel on the right.

Adding a DVD or CD-ROM Drive on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). If you want the drive to appear to the guest operating system as a SCSI drive, click the + sign beside **SCSI Devices**. If you want the drive to appear to the guest operating system as an IDE drive, click the + sign beside **IDE Drives**.

2. Select a device that is shown as **Not Installed**.
3. From the **Device Type** drop-down list, choose **CD-ROM** to connect to a physical DVD or CD-ROM drive. Choose **CD-ROM Image** to connect to an ISO image file.
4. If you are connecting to a physical drive, enter its device name (for example, `/dev/hdc`) in the **Name** field or click **Choose** to navigate to the name.

   If you are connecting to an ISO image file, enter the path and filename in the **Name** field or click **Choose** to navigate to the name.
5. Click **Install** to create the new DVD or CD-ROM drive, then click **OK** to save the configuration and close the Configuration Editor.

Adding Floppy Drives to a Virtual Machine

You can add floppy drives to your virtual machine, to a total of two floppy drives. A virtual floppy drive can connect to a physical floppy drive on the host computer, to an existing floppy image file or to a blank floppy image file.

Adding a Floppy Drive on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and click **Add** to start the Add Hardware Wizard.
2. Click **Floppy Drive**, then click **Next**.
3. Select what you want to connect to — a physical floppy drive on the host computer, an existing floppy image file or a new floppy image file. Click **Next**.
4. Select **Use a physical floppy drive**, choose the drive's letter from the drop-down list, then click **Finish**.

Adding a Floppy Drive on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). Click the **+** sign beside **Floppy Drives**.
2. Select a device that is shown as **Not Installed**.
3. On the **Type** drop-down list, choose **Device** to connect to a physical floppy drive on the host computer.

   Choose **File** from the drop-down list to connect to a floppy image file.
4. If you chose **Device**, accept the default device name shown (for example, `/dev/fd1` for the second physical floppy drive), type in the path and device name or click **Choose** to navigate to the device name.

   If you chose **File**, type in the path and filename for the floppy image file or click **Choose** to navigate to the file.

5. Click **Install** to install the new floppy drive, then click **OK** to save the configuration and close the Configuration Editor.

Connecting a CD-ROM or Floppy Drive to an Image File

You can use the Configuration Editor to connect an existing virtual CD-ROM or floppy drive to an image file.

You can connect a virtual CD-ROM drive to an ISO image file.

Connecting to an ISO Image File on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and select the DVD/CD-ROM drive you want to connect to the image file.
2. Select **Use ISO Image** and enter the path and filename for the image file or click **Browse** to navigate to the file.
3. Click **OK** to save the configuration and close the Configuration Editor.

Connecting to an ISO Image File on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). If your DVD/CD-ROM drive is configured as a SCSI drive, click the + sign beside **SCSI Devices**. If it is configured as an IDE drive, click the + sign beside **IDE Drives**.
2. Select the DVD/CD-ROM drive you want to connect to the image file and enter the path and filename in the **Name** field or click **Choose** to navigate to the name.
3. Click **OK** to save the configuration and close the Configuration Editor.

Connecting to a Floppy Image File on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and select the floppy drive you want to connect to an image file.
2. To use an existing floppy image, select **Use a floppy image**, type the path and filename for the floppy image file you want to use or click **Browse** to navigate to the file, then click **Finish**.

   To create a new image file, select **Create a blank floppy image.** Use the default path and filename or type in a new one. To navigate to a location, click **Browse**. When the field contains the path and filename you want to use for the new floppy image file, click **Finish**.

Connecting to a Floppy Image File on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). Click the + sign beside **Floppy Drives**.

2. Select the device you want to use.
3. On the **Type** drop-down list, choose **File**.
4. Type in the path and filename for the floppy image file or click **Choose** to navigate to the file.
5. Click **OK** to save the configuration and close the Configuration Editor.

Installing an Operating System onto a Raw Partition from a Virtual Machine

In some situations, you may want to install a guest operating system directly on a physical disk or partition — known as a raw disk — even if you do not need to boot that disk on the host, outside of the virtual machine.

It is possible to use either an unused partition or a completely unused disk on the host as a disk in the virtual machine. However, it is important to be aware that an operating system installed in this setting probably cannot boot outside of the virtual machine, even though the data is available to the host.

The instructions in this section do not apply to a disk with a previously installed operating system.

As with virtual disks, raw disks can be used in persistent, undoable and nonpersistent modes. For details on these modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 368.

Caution: Raw disks are an advanced feature and should be configured only by expert users.

GSX Server uses description files to control access to each raw disk on the system. These description files contain access privilege information that controls a virtual machine's access to certain partitions on the disks. This mechanism prevents users from accidentally running the host operating system again as a guest or running a guest operating system that the virtual machine is not configured to use. The description file also prevents accidental writes to raw disk partitions from badly behaved operating systems or applications.

Use the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) to configure a virtual machine to use existing raw disk partitions. The wizard guides you though creating a configuration for a new virtual machine including configuring the raw disk description files. Rerun the wizard to create a separate configuration for each guest operating system installed on a raw partition.

Note: While installing the guest operating system on a raw disk, if your virtual machine does not boot from the CD-ROM, try changing the boot order in the virtual machine's BIOS. Restart the virtual machine, then press F2 while the virtual machine is booting to enter the BIOS. Change the boot order there.

Configuring a Windows Host

Configuring the Virtual Machine to Use a Raw Disk

Use the following steps to run a guest operating system from a raw disk.

Note: If you use a Windows host's IDE disk in a raw disk configuration, it cannot be configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

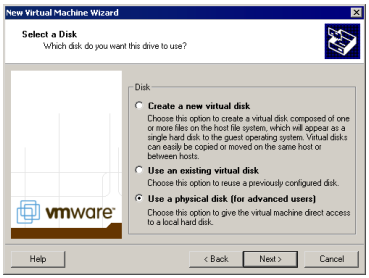
1. Identify the raw partition where the guest operating system will be installed.

   Check the guest operating system documentation regarding the type of partition on which the operating system can be installed. For example, operating systems like DOS, Windows 95 and Windows 98 must be installed on the first primary partition while others, like Linux, can be installed to a primary or extended partition on any part of the drive.

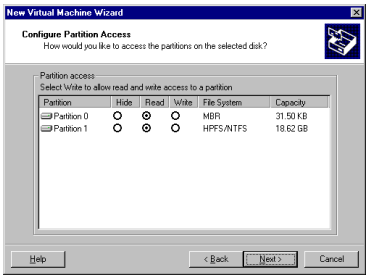
   Identify an appropriate raw partition or disk for the guest operating system to use. Check that the raw partition is not mounted by the Windows host and not in use by others. Also, be sure the raw partition or disk does not have data you will need in the future; if it does, back up that data now.

2. Start the New Virtual Machine Wizard (**File** > **New**) and select **Custom**.

3. When you reach the Select a Disk step, select **Use a physical disk**.


New Virtual Machine Wizard
Select a Disk
Which disk do you want this drive to use?
Disk
Create a new virtual disk
Choose this option to create a virtual disk composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk.
vmware
Help
< Back
Next >
Cancel

4. The next panel allows you to specify the access that is needed for each partition on the disk(s). Most partitions should be set to **Read**, and the partition that the virtual machine is to use should be set to **Write**.



Caution: Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted under Windows. Since the virtual machine and guest operating system access a raw disk partition while the host continues to run Windows, it is critical that you not allow the virtual machine to modify any partition mounted by the host or in use by another virtual machine. To safeguard against this problem, be sure the raw disk partition you mark as **Write** for the virtual machine is not in use.

5. The partition where you are installing the guest operating system should be unmapped in the host.

   On a Windows Server 2003 or Windows 2000 host, use Disk Management (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management**). Select the partition to unmap, then choose **Action** > **All Tasks** > **Change Drive Letter and Path**, then click **Remove**.

   On a Windows NT host, use the Disk Administrator (**Start** > **Programs** > **Administrative Tools**). First highlight the partition that contains the guest operating system, then choose **Tools** > **Assign Drive Letter**. In this form, select **Do not assign a drive letter** for the partition and click **OK**. The unmapping happens immediately.

6. Use the Configuration Editor (**Settings** > **Configuration Editor**) if you want to change any configuration options from the wizard defaults — for example, to change the amount of memory allocated to the guest or to change disk modes.

7. At this point you are ready to begin installing the guest operating system onto the raw disk you configured for the virtual machine. For more details, read the installation notes for various guest operating systems in Installing Guest Operating Systems on page 251.

Configuring a Linux Host

1. Identify the raw partition where the guest operating system will be installed.

   Check the guest operating system documentation regarding the type of partition on which the operating system can be installed. For example, operating systems like DOS, Windows 95 and Windows 98 must be installed on the first primary partition while others, like Linux, can be installed to a primary or extended partition on any part of the drive.

   Identify an appropriate raw partition or disk for the guest operating system to use. Check that the raw partition is not mounted by the Linux host and not in use by others. Also, be sure the raw partition or disk does not have data you will need in the future; if it does, back up that data now.

2. Check the operating system partition mounts. Be sure the existing disk partitions that you plan to configure the virtual machine to use are not mounted by Linux.

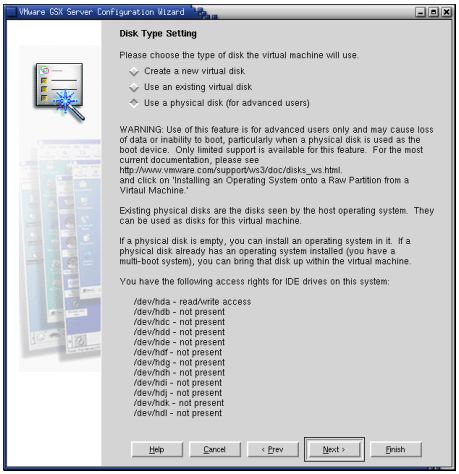
3. Set the device group membership or device ownership.

   The master raw disk device or devices need to be readable and writable by the user who runs GSX Server. On most distributions, the raw devices, such as `/dev/hda` (IDE raw disk) and `/dev/sdb` (SCSI raw disk) belong to group-id `disk`. If this is the case, you can add GSX Server users to the `disk` group. Another option is to change the owner of the device. Please think carefully of security in exploring different options here.

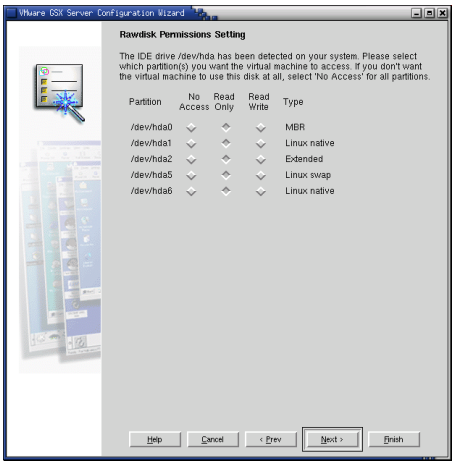
   It is a good idea to grant GSX Server users access to all `/dev/hd[abcd]` raw devices that contain operating systems or boot managers and then rely on GSX Server's raw disk configuration files to guard access. This provides boot managers access to configuration and other files they may need to boot the operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that may be on another drive.

4. Run the Configuration Wizard (**File** > **Wizard**).

5. When you reach the Disk Type Settings panel, select **Use a physical disk**. Click **Next**.


VMware GSX Server Configuration Wizard
Disk Type Setting
Please choose the type of disk the virtual machine will use.
Create a new virtual disk
Use an existing virtual disk
Use a physical disk (for advanced users)
WARNING: Use of this feature is for advanced users only and may cause loss of data or inability to boot, particularly when a physical disk is used as the boot device. Only limited support is available for this feature. For the most current documentation, please see http://www.vmware.com/support/ws3/doc/disks_ws.html, and click on 'Installing an Operating System onto a Raw Partition from a Virtaul Machine.'
Existing physical disks are the disks seen by the host operating system. They can be used as disks for this virtual machine.
If a physical disk is empty, you can install an operating system in it. If a physical disk already has an operating system installed (you have a multi-boot system), you can bring that disk up within the virtual machine.
You have the following access rights for IDE drives on this system:
/dev/hda - read/write access
/dev/hdb - not present
/dev/hdc - not present
/dev/hdd - not present
/dev/hde - not present
/dev/hdf - not present
/dev/hdg - not present
/dev/hdh - not present
/dev/hdi - not present
/dev/hdj - not present
/dev/hdk - not present
/dev/hdl - not present
Help
Cancel
< Prev
Next >
Finish

6. Select the read/write option only for the raw partition or disk (and its master boot record) on which you want to install the guest operating system. If the raw disk you plan to use has multiple partitions already on it, be aware that certain operating systems (DOS, Windows 95, Windows 98) must be installed on the first primary partition.


VMware GSX Server Configuration Wizard
Rawdisk Permissions Setting
The IDE drive /dev/hda has been detected on your system. Please select which partition(s) you want the virtual machine to access. If you don't want the virtual machine to use this disk at all, select 'No Access' for all partitions.
Partition
No Access
Read Only
Read Write
Type
/dev/hda0 MBR
/dev/hda1 Linux native
/dev/hda2 Extended
/dev/hda5 Linux swap
/dev/hda6 Linux native
Help
Cancel
< Prev
Next >
Finish

Caution: Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted under Linux. Since the virtual machine and guest operating system access an existing partition while the host continues to run Linux, it is critical that the virtual machine not be allowed to modify any partition mounted by the host or in use by another virtual machine. To safeguard against this problem, be sure the partition you mark read/write for the virtual machine is not mounted under the Linux host.

7. Complete the remaining steps in the wizard. On the review screen, note the path to the configuration (`.cfg`) file. You will need it in the next step.
8. Start a local console and manually change the controller/channel assignment selected by the wizard. Type `vmware -G <config-file>.cfg`, where `<config-file>` is the path to the configuration file created by the wizard.
9. Choose **Settings** > **Configuration Editor** and check that your IDE configuration specifies at least two raw disk description files. These files are named `<configuration-name>.hda`, `<configuration-name>.hdb` and so on.
10. Identify the description file for the raw disk to which you will install the new guest operating system. For example, if your physical machine has an unused disk on the secondary master IDE channel and you want to use this device for the virtual machine, you should see a file called `<configuration-name>.hdc` next to the virtual machine's IDE 1:0 or S-M configuration entry.
11. Replace the name of the description file (`.hda` file) next to the virtual machine's IDE 0:0 channel with the name of the description file you identified in the previous step.
12. Remove the other raw disk description file(s) from the virtual machine's IDE configuration dialog box and click **OK**.
13. Click **OK** to save the changes and close the Configuration Editor.
14. At this point you are ready to begin installing the guest operating system on the raw disk you configured for the virtual machine. For more details, read the installation notes for various guest operating systems in Installing Guest Operating Systems on page 251.

Disk Performance in Windows NT Guests on Multiprocessor Hosts

Some users have seen slower than expected disk input/output performance when running Windows NT as a guest operating system in a virtual machine using IDE virtual disks on a multiprocessor host computer. The I/O issue is especially noticeable when the virtual machine is booting.

Improving Performance

You may increase performance by enabling DMA (direct memory access) on the virtual hard disk's IDE channel in the virtual machine.

Note: You should not enable DMA on the IDE channel to which you have attached your virtual DVD/CD-ROM drive. In most cases, the virtual hard disk is attached to IDE channel 0 and the virtual DVD/CD-ROM drive is attached to IDE channel 1, so this is not an issue.

If you have a virtual disk and a DVD/CD-ROM attached as master and slave to the primary IDE controller (channel 0) and you want to enable DMA, power off the virtual machine and use the Configuration Editor (**Settings** > **Configuration Editor**) to move the DVD/CD-ROM drive to the secondary IDE controller (channel 1) at IDE 1:0.

You can enable the DMA feature after you finish installing Windows NT. You must install Service Pack 3 or higher in the virtual machine to enable this option.

Once the virtual machine is running Windows NT, insert the Service Pack 3 or Service Pack 4 CD in the drive and run `DMACHECK.EXE` from the `\SUPPORT\UTILS\I386` folder on the CD. Or download `DMACHECK.EXE` from the Microsoft Web site (*support.microsoft.com/support/kb/articles/Q191/7/74.ASP*).

Click the **Enabled** option for the IDE controller and channel configured for the virtual disk. Typically, this is channel 0 only, unless you have the virtual machine configured with multiple virtual disks and no virtual DVD/CD-ROM drive.

As noted above, you should not enable DMA on an IDE channel with a virtual DVD/CD-ROM drive attached.

12

Networking

Configuring Your Virtual Network

VMware GSX Server provides virtual networking components that let you create a wide range of configurations.

You can choose the most common configurations — bridged networking, network address translation (NAT) and host-only networking — in the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) when you create a virtual machine. The wizard then connects the proper components for you automatically.

You can set up more specialized configurations by choosing the appropriate settings in the Configuration Editor and on your host computer.

On a Windows host, the software needed for all networking configurations is installed when you install GSX Server. On a Linux host, all components are available if you choose to have both bridged and host-only networking available to your virtual machines at the time you install GSX Server.

The first sections of this chapter give you a quick look at the virtual networking components that GSX Server provides and show how you can use them with your virtual machine. The rest of the chapter provides more detail on some networking capabilities and specialized configurations.

- Components of the Virtual Network on page 406
- Common Networking Configurations on page 408
  - Bridged Networking on page 408
  - Network Address Translation (NAT) on page 409
  - Host-Only Networking on page 411
- Custom Networking Configurations on page 412
- Changing the Networking Configuration on page 415
  - Adding and Modifying Virtual Network Adapters on page 415
  - Configuring Bridged Networking Options on a Windows Host on page 417
  - Disabling and Removing NAT and Host-Only Adapters on page 420
- Advanced Networking Topics on page 423
  - Selecting IP Addresses on a Host-Only Network or NAT Configuration on page 423
  - Avoiding IP Packet Leakage in a Host-Only Network on page 427

- Changing the MAC Address of a Virtual Machine on page 428
- Controlling Routing Information for a Host-Only Network on a Linux Host on page 429
- Other Potential Issues with Host-Only Networking on a Linux Host on page 429
- Using Samba for File Sharing on a Linux Host on page 431
- Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems on page 441
- Configuring a Virtual Machine to Switch Network Adapters on a Windows NT Host on page 439
- Configuring Bridged Networking when Using Teamed Network Interface Cards on Your Host on page 445
- Setting Up a Second Bridged Network Interface on a Linux Host on page 446
- Setting Up Two Separate Host-Only Networks on page 447
- Routing between Two Host-Only Networks on page 452
- Using Virtual Ethernet Adapters in Promiscuous Mode on a Linux Host on page 457

- Understanding NAT on page 458
  - Using NAT in GSX Server on page 458
  - The Host Computer and the NAT Network on page 458
  - DHCP on the NAT Network on page 459
  - DNS on the NAT Network on page 459
  - External Access from the NAT Network on page 459
  - Advanced NAT Configuration on page 461
  - Considerations for Using NAT on page 463
  - Using NAT with NetLogon (Windows Hosts and Virtual Machines Only) on page 464
  - Sample Windows vmnetnat.conf File on page 466

Components of the Virtual Network

Virtual Switch — Like a physical switch, a virtual switch lets you connect other networking components together. Virtual switches are available if you have installed GSX Server with any networking options (bridged, NAT or host-only). They are created as needed by the GSX Server software, up to a total of 9 switches on a Windows host and 99 switches on a Linux host. You can connect one or more virtual machines to a switch.

A few of the switches have special names. One is named Bridged (also called VMnet0). It is used in the standard bridged networking configuration. Another is named Host-only (also called VMnet1). It is used in the standard host-only configuration. A third is named NAT (also called VMnet8). It is used in the standard network address translation configuration. The others are simply named VMnet2, VMnet3, VMnet4 and so on.

You connect a virtual machine to a switch by selecting the name of the switch you want in the Configuration Editor, using the panel that configures the virtual network adapter you want to connect to the switch.

Bridge — The bridge lets you connect your virtual machine to the LAN used by your host computer. It connects the virtual network adapter in your virtual machine to the physical Ethernet adapter in your host computer.

The bridge is installed during GSX Server installation (on a Linux host, you must choose to make bridged networking available to your virtual machines). It is set up automatically when you create a new virtual machine using bridged networking.

Additional virtual bridges can be set up for use in custom configurations that require connections to more than one LAN through more than one physical Ethernet adapter on the host computer.

Host-only adapter — The host-only adapter is a virtual Ethernet adapter that appears to your host operating system as VMware Virtual Ethernet Adapter on a Windows host and as the Host-Only Interface on a Linux host. It allows you to communicate between your host computer and the virtual machines on that host computer. It is not connected to any external network unless you set up special software on the host computer — a proxy server, for example — to connect the host-only adapter to the physical network adapter.

The software that creates the host-only adapter is installed when you install GSX Server (on a Linux host, you must choose to make host-only networking available to your virtual machines). A host-only adapter is then created automatically when you boot the host computer.

Additional host-only adapters can be set up for use in custom configurations that need them.

NAT device — The NAT (network address translation) device allows you to connect your virtual machines to an external network in situations where you have only one IP address, and that address is used by the host computer. You can, for example, use NAT to connect your virtual machines to the Internet through a dial-up connection on the host computer or through the host computer's Ethernet adapter, wireless Ethernet adapter or Token Ring card.

The NAT device is set up automatically if you choose NAT as the networking option when you set up a virtual machine.

DHCP server — The DHCP (dynamic host configuration protocol) server provides IP network addresses to virtual machines in host-only and NAT configurations.

Network adapter — One virtual network adapter is set up for your virtual machine when you create it with the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) using any type of networking. It appears to the guest operating system as an AMD PCNET PCI adapter.

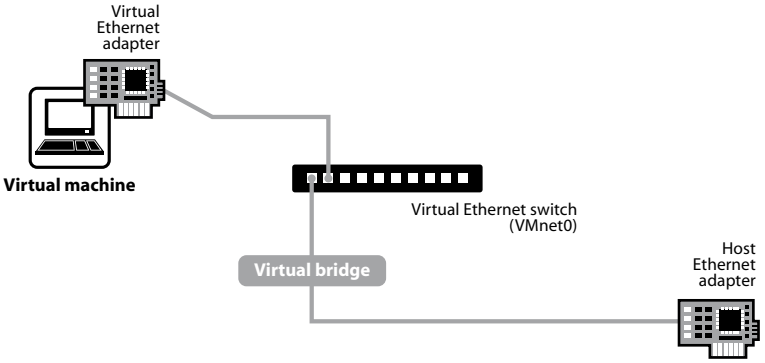
You can create and configure up to three virtual network adapters in each virtual machine using the Configuration Editor.

Common Networking Configurations

These sections illustrate the networking configurations that are set up for you automatically when you choose the standard networking options in the New Virtual Machine Wizard (on Windows hosts), Configuration Wizard (on Linux hosts) or Configuration Editor (on Windows or Linux hosts).

Only one virtual machine is shown in each example, but multiple virtual machines can be connected to the same virtual Ethernet switch. On a Windows host, you can connect an unlimited number of virtual network devices to a virtual switch. On a Linux host, you can connect up to 32 devices.

Bridged Networking



Bridged networking connects a virtual machine to a network using the host computer's Ethernet adapter.

Bridged networking is set up automatically if you select **Use bridged networking** in the New Virtual Machine Wizard on Windows hosts or **Bridged networking** in the Configuration Wizard on Linux hosts. On a Linux host, this selection is available only if you enable networking when you install GSX Server.

If your host computer is on an Ethernet network, this is often the easiest way to give your virtual machine access to that network.

If you use bridged networking, your virtual machine needs to have its own identity on the network. For example, on a TCP/IP network, the virtual machine needs its own IP address. Your network administrator can tell you whether IP addresses are available for your virtual machine and what networking settings you should use in the guest operating system. Generally, your guest operating system may acquire an IP address and other network details automatically from a DHCP server, or you may need to set the IP address and other details manually in the guest operating system.

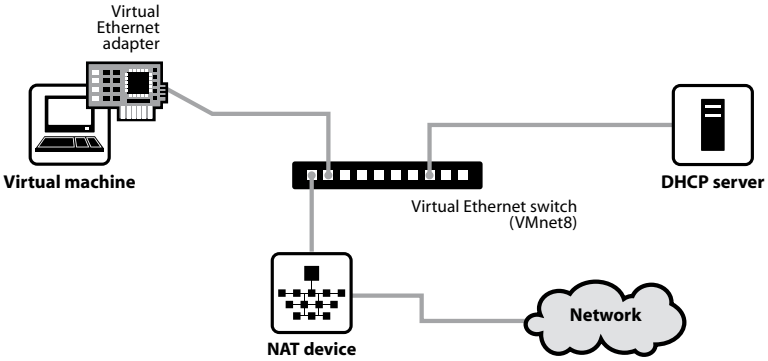
If you use bridged networking, the virtual machine is a full participant in the network. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network.

Be aware that if the host computer is set up to boot multiple operating systems and you run one or more of them in virtual machines, you need to configure each operating system with a unique network address. People who boot multiple operating systems often assign all systems the same address, since they assume only one operating system will be running at a time. If you use one or more of the operating systems in a virtual machine, this assumption is no longer true.

If you make some other networking selection in the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) and later decide you want to use bridged networking, you can make that change in the Configuration Editor (**Settings** > **Configuration Editor**). For details, see Changing the Networking Configuration on page 415.

Note: You cannot use bridged networking if your host has a wireless NIC installed. If you want to run virtual machines on a host that uses wireless NICs, you need to configure your virtual machines to use NAT.

Network Address Translation (NAT)



NAT gives a virtual machine access to network resources using the host computer's IP address.

A network address translation connection is set up automatically if you select **Use network address translation** in the New Virtual Machine Wizard on Windows hosts or **NAT** in the Configuration Wizard on Linux hosts.

If you want to connect to the Internet or other TCP/IP network using the host computer's dial-up networking connection and you are not able to give your virtual

machine an IP address on the external network, NAT is often the easiest way to give your virtual machine access to that network.

NAT also allows you to connect to a TCP/IP network using a wireless LAN adapter or Token Ring adapter on the host computer.

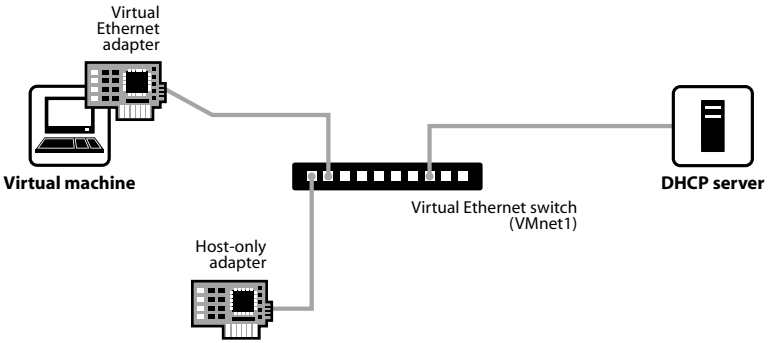
If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

If you select NAT, the virtual machine can use many standard TCP/IP protocols to connect to other machines on the external network. For example, you can use HTTP to browse Web sites, FTP to transfer files and Telnet to log on to other computers. In the default configuration, computers on the external network cannot initiate connections to the virtual machine. That means, for example, that the default configuration does not let you use the virtual machine as a Web server to send Web pages to computers on the external network.

If you make some other networking selection in the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) and later decide you want to use NAT, you can make that change in the Configuration Editor (**Settings** > **Configuration Editor**). For details, see Changing the Networking Configuration on page 415.

For a more thorough discussion of NAT, see Understanding NAT on page 458.

Host-Only Networking



Host-only networking creates a network that is completely contained within the host computer.

A host-only network is set up automatically if you select **Use Host-Only Networking** in the New Virtual Machine Wizard on Windows hosts or **Host-Only Networking** in the Configuration Wizard on Linux hosts. On Linux hosts, this selection is available only if you enabled host-only networking when you installed GSX Server.

Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual Ethernet adapter that is visible to the host operating system. This approach can be very useful if you need to set up an isolated virtual network.

If you install the proper routing or proxy software on your host computer, you can establish a connection between the host-only virtual Ethernet adapter and a physical network adapter on the host computer. This allows you, for example, to connect the virtual machine to a Token Ring or other non-Ethernet network.

On a Windows 2000 or Windows Server 2003 host computer, you can use host-only networking in combination with the Internet connection sharing feature in Windows to allow a virtual machine to use the host's dial-up networking adapter or other connection to the Internet.

If you use host-only networking, your virtual machine and the host-only adapter are connected to a private TCP/IP network. Addresses on this network are provided by the VMware virtual DHCP server.

If you make some other networking selection in the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) and later decide you want to use host-only networking, you can make that change in the Configuration Editor (**Settings** > **Configuration Editor**). For details, see Changing the Networking Configuration on page 415.

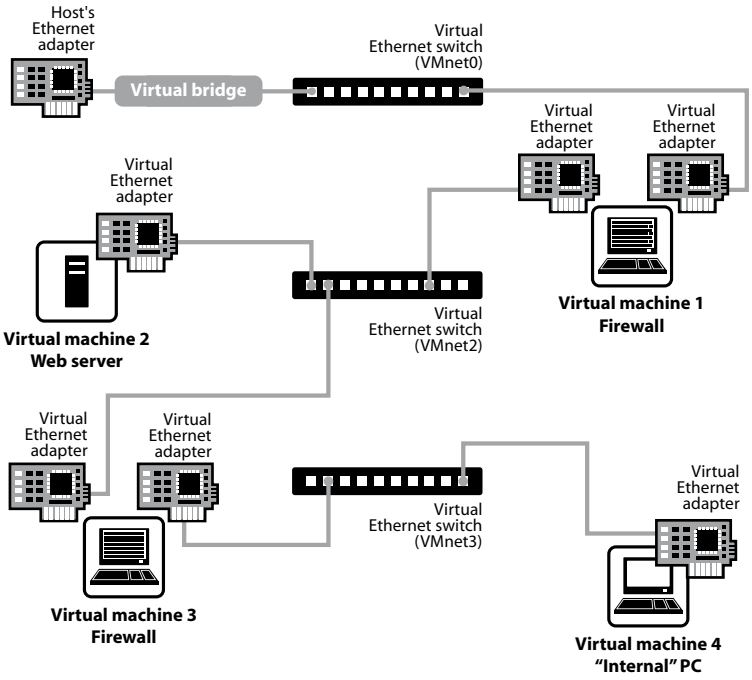
Custom Networking Configurations

The virtual networking components provided by GSX Server make it possible for you to create sophisticated virtual networks. The virtual networks can be connected to one or more external networks, or they may run entirely on the host computer.

Setting up networking components for your custom virtual network is a straightforward process. Before attempting to set up complex virtual networks, you should have a good understanding of how to configure network devices in your host and guest operating systems.

The sample configuration described in this section illustrates many of the ways you can combine devices on a virtual network. Other custom configurations are described in Advanced Networking Topics on page 423 and Understanding NAT on page 458.

.



In this custom configuration, a Web server connects through a firewall to an external network. An administrator's computer can connect to the Web server through a second firewall.

To set up this configuration, you must create four virtual machines and use the Configuration Editor to adjust the settings for their virtual Ethernet adapters. You also need to install the appropriate guest operating systems and application software in each virtual machine and make the appropriate networking settings in each virtual machine.

1. Set up four virtual machines using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

   Create the first virtual machine with bridged networking so it can connect to an external network using the host computer's Ethernet adapter.

   Create the other three virtual machines without networking. You will set up their virtual Ethernet adapters in later steps.

2. Start a console and open virtual machine 1. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a second virtual network adapter, as described in Changing the Networking Configuration on page 415. Connect the second adapter to **Custom (VMnet2)**.

   Click **OK** to save the configuration and close the Configuration Editor.

3. Start a console and open virtual machine 2. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet2)**.

   Click **OK** to save the configuration and close the Configuration Editor.

4. Start a console and open virtual machine 3. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet2)**.

   Use the Configuration Editor to add a second virtual network adapter. Connect the adapter to **Custom (VMnet3)**.

   Click **OK** to save the configuration and close the Configuration Editor.

5. Start a console and open virtual machine 4. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet3)**.

   Click **OK** to save the configuration and close the Configuration Editor.

6. Determine the network addresses used for VMnet2 and VMnet3.

   On a Windows host, open a command prompt on the host computer and run `ipconfig /all`. Note the network addresses used by each virtual switch.

   On a Linux host, run `ifconfig` at the console or in a terminal window on the host computer. Note the network addresses used by each virtual switch.

7. Start a console and open each virtual machine in turn and install the appropriate guest operating system.

8. Configure the networking in each guest operating system.

   For the bridged Ethernet adapter in virtual machine 1, use the networking settings needed for a connection to the external network. If the virtual machine gets its IP address from a DHCP server on the external network, the default settings should work.

   For the second Ethernet adapter in virtual machine 1, manually assign an IP address in the range you have decided to use with VMnet2.

   In virtual machine 2, assign an IP address in the range you have decided to use with VMnet2.

   In virtual machine 3, network adapters are connected to VMnet2 and VMnet3. Assign each adapter an IP address in the range you have decided to use with the virtual switch to which it is connected.

   In virtual machine 4, assign an IP address in the range you have decided to use with VMnet3.

9. Install the necessary application software in each virtual machine.

Changing the Networking Configuration

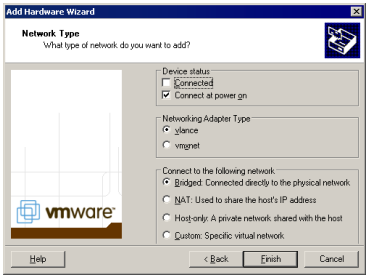
Using the Configuration Editor, you can add virtual Ethernet adapters to your virtual machine and change the configuration of existing adapters.

Adding and Modifying Virtual Network Adapters

Windows Hosts

To add a new virtual Ethernet adapter, follow these steps.

1. Be sure the virtual machine to which you want to add the network adapter is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Click **Add**.
4. The Add Hardware Wizard starts. Select **Network Adapter**. Click **Next**.



5. For Windows 2000, Windows XP and Windows Server 2003 virtual machines, select the network driver to use. Choose from `vlance`, the default, or `vmxnet`, which provides better performance. The difference in network performance is most noticeable if the virtual machine is connected to a Gigabit Ethernet card.
6. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
7. If you select **Custom**, choose the VMnet virtual switch you want to use for the network from the drop-down list.

   Note: Although VMnet0, VMnet1 and VMnet8 are available in this list, they are normally used for bridged, host-only and NAT configurations, respectively. Special steps are required to make them available for use in custom configurations. You should choose one of the other switches.
8. Click **Finish**. The new adapter is added.
9. Click **OK** to save your configuration and close the Configuration Editor.

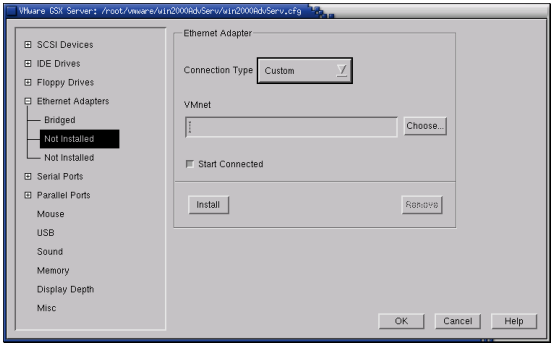
To change the configuration of an existing virtual network adapter, follow these steps.

1. Be sure the virtual machine with the adapter you want to modify is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Select the adapter you want to modify.
4. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
5. If you select **Custom**, choose the VMnet virtual switch you want to use for the network from the drop-down list.
6. Click **OK** to save your changes and close the Configuration Editor.

Linux Hosts

To add a new virtual Ethernet adapter, follow these steps.

1. Be sure the virtual machine to which you want to add the network adapter is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Click the **+** sign beside **Network Adapters**.
4. Select an adapter that is listed as **Not Installed**.



5. From the drop-down list, choose the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
6. If you choose **Custom**, enter the path to the VMnet virtual switch you want to use in the VMnet field. For example, if you want to use VMnet2, type `/dev/vmnet2`.
7. Click **Install** to install the new adapter.
8. Click **OK** to save your configuration and close the Configuration Editor.

To change the configuration of an existing virtual network adapter, follow these steps.

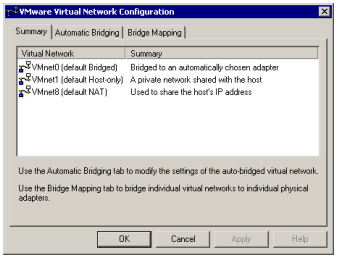
1. Be sure the virtual machine with the adapter you want to modify is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Click the + sign beside **Network Adapters**.
4. Select the adapter you want to modify.
5. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
6. If you choose custom, enter the number of the VMnet virtual switch you want to use in the VMnet field. For example, if you want to use VMnet2, type `/dev/VMnet2`.
7. Click **OK** to save your changes and close the Configuration Editor.

Configuring Bridged Networking Options on a Windows Host

You can view and change the settings for bridged networking on your host. These changes affect all virtual machines using bridged networking on the host.

You can decide which NICs on your host to use for bridged networking. You can map specific NICs to specific virtual networks (VMnets).

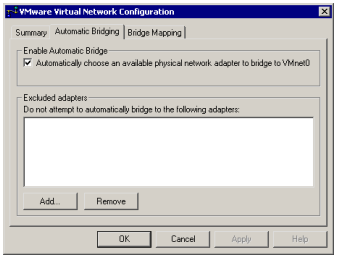
1. Open a local console.
2. Choose **Settings** > **Manage Virtual Networks**.
3. The VMware Virtual Network Configuration dialog box appears, with the **Summary** tab active. By default, the VMnet0 virtual switch is set up in bridged mode and bridges to one of the active Ethernet adapters on the host computer.


VMware Virtual Network Configuration
Summary
Automatic Bridging
Bridge Mapping
Virtual Network
Summary
VMnet0 (default Bridged)
Bridged to an automatically chosen adapter
VMnet1 (default Host-only)
A private network shared with the host
VMnet8 (default NAT)
Used to share the host's IP address
Use the Automatic Bridging tab to modify the settings of the auto-bridged virtual network.
Use the Bridge Mapping tab to bridge individual virtual networks to individual physical adapters.
OK
Cancel
Apply
Help

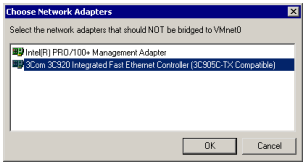
The choice of which adapter it uses is arbitrary. You can restrict the range of choices using options on the **Automatic Bridging** tab.

(Also shown are VMnet1, the default virtual switch for host-only networking, and VMnet8, the default virtual switch for NAT, if they are enabled in GSX Server.)

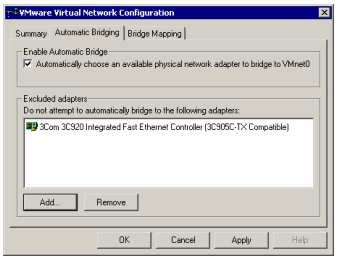
4. To exclude one or more physical Ethernet adapters from the list to which VMnet0 may be bridged, click the **Automatic Bridging** tab. To exclude an Ethernet adapter, click **Add** to add it to the list of excluded devices.



In the Choose Network Adapters dialog box, select the listing for the adapter you want to exclude, then click **OK**.

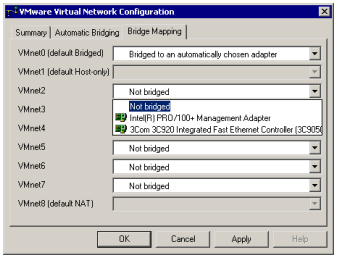

Choose Network Adapters
Select the network adapters that should NOT be bridged to VMnet0
Intel(R) PRO/100+ Management Adapter
3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)
OK
Cancel

To remove an adapter from the list of excluded adapters, select its name in the list, then click **Remove**.



5. To designate a physical Ethernet adapter to be used for bridged networking on virtual switches named VMnet2 through VMnet7, click the **Bridge Mapping** tab.

Choose an adapter from the drop-down list beside the name of the virtual switch you want to use.



Caution: Be careful when you change the bridged adapter mappings. If you re-assign a physical Ethernet adapter to a different virtual switch, any virtual machine using the original switch loses its network connectivity via that switch. You must then change the setting for each affected virtual machine's network adapter individually. This can be especially troublesome if your host has only one physical Ethernet adapter and you reassign it to a VMnet other than VMnet0; even though the VMnet still appears to be bridged to an automatically chosen adapter, the only adapter it can use has been assigned to another VMnet.

6. When you have made all the changes you want to make on all panels of the VMware Virtual Network Configuration dialog box, click **OK**.

Disabling and Removing NAT and Host-Only Adapters

When you install GSX Server, two network adapters are added to the configuration of your host operating system — one that allows the host to connect to the host-only network and one that allows the host to connect to the NAT network.

If you are not using these adapters, you may wish to remove them (users on Windows hosts can choose to disable the adapters instead of removing them). The presence of these adapters has a slight performance cost, because broadcast packets must go to the extra adapters. On Windows networks, browsing your network may be slower than usual. And in some cases, these adapters interact with the host computer's networking configuration in undesirable ways.

Disabling a Host-only or NAT Adapter on a Windows Host

Windows Server 2003 Hosts

1. Choose **Start** > **Settings** > **Control Panel**.
2. Double-click **Network and Dial-up Settings**.
3. Right-click the VMware Virtual Ethernet Adapter you want to disable. The host-only adapter is VMnet1; the NAT adapter is VMnet8.
4. In the pop-up menu, choose **Properties**.
5. Click **Configure**.
6. In the **Device Usage** pull-down list choose **Disable from this HW profile**.

Windows 2000 Hosts

1. Choose **Start** > **Settings** > **Network and Dial-up Connections**.
2. Right-click the VMware Virtual Ethernet Adapter you want to disable. The host-only adapter is VMnet1; the NAT adapter is VMnet8.
3. In the pop-up menu, select **Disable**.

Windows NT Hosts

1. Choose **Start** > **Settings** > **Control Panel**.
2. Double-click **Network**.
3. Click the **Bindings** tab.
4. Choose **All adapters**.
5. Select the VMware Virtual Ethernet Adapter you want to disable. The host-only adapter is VMnet1; the NAT adapter is VMnet8. Click **Disable**.

Removing a Host-only or NAT Adapter on a Windows Host

1. Log on as a member of the Administrators group.
2. Open a command prompt.
3. Change to the GSX Server program folder.
   ```
   cd \Program Files\VMware\VMware GSX Server
   ```
4. Run the appropriate command to remove the adapter or adapters you want to uninstall.

   To remove the host adapter for the host-only network:
   ```
   vmware_netinstall -r *VMnet1
   ```
   To remove the host adapter for the NAT network:
   ```
   vmware_netinstall -r *VMnet8
   ```
   To remove all host-only adapters:
   ```
   vmware_netinstall -d
   ```
   When the last host-only adapter is uninstalled, the VMnetDHCP service is also uninstalled automatically.

To uninstall the NAT service, take the following steps.

1. Log on as a member of the Administrators group.
2. Open a command prompt.
3. Change to the host's `system32` folder.

   ```
   cd \WINNT\system32
   ```
   If your computer uses a different path for this folder, adjust the command appropriately.
4. Run the uninstall command.
   ```
   vmnat -Uninstall
   ```

Removing a Host-only or NAT Adapter on a Linux Host

1. Become root and run the GSX Server configuration program.

   ```
   su -
   vmware-config.pl
   ```

2. Watch for the following question:

   ```
   Do you want networking for your Virtual Machines?
   (yes/no/help) [yes]
   ```

   Answer Yes if you still want to use any networking in your virtual machines, then continue to the next question.

   Otherwise, answer No to remove all networking.

3. If you answer Yes, the program prompts you to select the wizard or editor to edit your network configuration.

   ```
   Would you prefer to modify your existing networking
   configuration using the wizard or the editor? (wizard/
   editor/help) [wizard] editor
   ```

   Select editor. This is the only way to delete virtual network adapters without removing all of them.

4. You see a list of virtual network adapters that have been configured. Select the adapter you wish to disable.

   ```
   The following virtual networks have been defined:

   . vmnet0 is bridged to eth0
   . vmnet1 is a host-only network on subnet 172.16.155.0.
   . vmnet8 is NAT network on a private subnet 172.16.107.0.

   Which virtual network do you wish to configure? (0-99) 1
   ```

5. You may be prompted to keep this virtual network. If you are sure you want to remove it, answer Yes to the question.

   ```
   The network vmnet1 has been reserved for a host-only
   network. You may change it, but it is highly recommended
   that you use it as a host-only network. Are you sure you
   want to modify it? (yes/no) [no] yes
   ```

6. When prompted about the type of virtual network, select None and the virtual network will be removed.

   ```
   What type of virtual network do you wish to set vmnet1?
   (bridged,hostonly,nat,none) [hostonly] none
   ```

Advanced Networking Topics

Selecting IP Addresses on a Host-Only Network or NAT Configuration

A host-only network uses a private virtual network. The host and all virtual machines configured for host-only networking are connected to the network through a virtual switch. Typically all the parties on this private network use the TCP/IP protocol suite, although other communication protocols may be used.

A network address translation (NAT) configuration also sets up a private network, which must be a TCP/IP network. The virtual machines configured for NAT are connected to that network through a virtual switch. The host computer is also connected to the private network used for NAT.

Each virtual machine and the host must be assigned addresses on the private network. This is typically done using the DHCP server that comes with GSX Server. Note that this server does not service virtual (or physical) machines residing on bridged networks.

Addresses can also be assigned "statically" from a pool of addresses that are not assigned by the DHCP server.

When host-only networking is enabled at the time GSX Server is installed, the network number to use for the virtual network is automatically selected as an unused private IP network number. To find out what network is used, run `ipconfig` from a command prompt on a Windows host or `ifconfig` on a Linux host.

A NAT configuration also uses an unused private network automatically selected when you install GSX Server. To check what network is used in a Windows Server 2003, Windows XP, Windows 2000 or Windows NT guest, run `ipconfig`. In a Windows Me or Windows 9x guest, run `winipcfg`. In a Linux guest, run `ifconfig`.

Using DHCP to assign IP addresses is simpler and more automatic than statically assigning them. Most Windows operating systems, for example, come preconfigured to use DHCP at boot time, so Windows virtual machines can connect to the network the first time they are booted, without additional configuration. If you want your virtual machines to communicate with each other using names instead of IP addresses, however, you must set up a naming convention, a name server on the private network, or both. In that case it may be simpler to use static IP addresses.

In general, if you have virtual machines you intend to use frequently or for extended periods of time, it is probably most convenient to assign them static IP addresses or

configure the VMware DHCP server to always assign the same IP address to each of these virtual machines.

Configuring the DHCP Server on a Linux Host

On a Linux host, you configure the host-only DHCP server by editing the DHCP configuration file for VMnet1 (`/etc/vmware/vmnet1/dhcp/dhcp.conf`). To configure the DHCP server for the NAT network, edit the configuration file for VMnet8 (`/etc/vmware/vmnet8/dhcp/dhcp.conf`).

Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. Consult the manual pages `dhcpd(8)` and `dhcpd.conf(8)`.

Configuring the DHCP Server on a Windows Host

Follow these steps to change the subnet of the DHCP server for the host-only network on VMnet1. In this example, you set the IP address of your host-only network to 192.168.3.1. To change the subnet used by a host-only DHCP server, you need to make the change to the IP address in two places: in the registry and in the `vmnetdhcp.conf` file.

1. Open the Windows registry.

   Choose **Start** > **Run**. Then type `regedit`.

2. Look for the registry key
   \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   VMnetDHCP\Parameters\VirtualEthernetSegments\1.

   In that key, there is a value with the name HostIpAddress. The data is a hexadecimal value corresponding to the IP address of the host. Change this hexadecimal value to that of the new IP address. For example, the registry may contain the value 01dea8c0. This corresponds to the IP address 192.168.222.1.
   c0 = 192
   a8 = 168
   de = 222
   01 = 1

   Notice that the hexadecimal number seems backwards — with the pairs of digits in the opposite order from the way they are usually given when you write an IP address.

   Change the value of this registry key to 0103a8c0, which corresponds to 192.168.3.1.

3. Find the file `vmnetdhcp.conf` in the system directory. On most systems, this will be `C:\WINNT\system32\vmnetdhcp.conf`. Look for the text `Virtual ethernet segment 1` in the file. Sample text from the file:

```
# Virtual ethernet segment 1
# Added at 07/05/01 14:30:18
subnet 192.168.222.0 netmask 255.255.255.0 {
range 192.168.222.128 192.168.222.254; # up to 126 VMs
option broadcast-address 192.168.222.255;
option domain-name-servers 192.168.222.1;
option domain-name "localdomain";
}
host VMnet1 {
hardware ethernet 00:50:56:C0:00:01;
fixed-address 192.168.222.1;
option domain-name-servers 0.0.0.0;
option domain-name "";
}
```

   Replace all instances of the old IP address — 192.168.222.1 — with the new IP address — 192.168.3.1 — as shown below.

```
# Virtual ethernet segment 1
# Added at 07/05/01 14:30:18
subnet 192.168.3.0 netmask 255.255.255.0 {
range 192.168.3.128 192.168.3.254; # up to 126 VMs
option broadcast-address 192.168.3.255;
option domain-name-servers 192.168.3.1;
option domain-name "localdomain";
}
host VMnet1 {
hardware ethernet 00:50:56:C0:00:01;
fixed-address 192.168.3.1;
option domain-name-servers 0.0.0.0;
option domain-name "";
}
```

4. Reboot the host computer so the new settings will take effect.

To make corresponding changes to the DHCP server for the NAT network, follow the same procedure, with these changes:

- Edit the registry key \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VMnetDHCP\Parameters\VirtualEthernetSegments\8.

- In `vmnetdhcp.conf`, edit the sections that begin with
  `# Virtual ethernet segment 8`
  and
  `host VMnet8 {`

Choosing the Method for Assigning IP Addresses

For virtual machines that you do not expect to keep for long, use DHCP and let it allocate an IP address.

For each host-only network, the available IP addresses are split up using the conventions shown in the table below, where <net> is the network number assigned to your host-only network. GSX Server always uses a Class C address for host-only and NAT networks.

Address Use on a Host-Only Network

Range	Address use	Example
<net>.1	Host machine	192.168.0.1
<net>.2–<net>.127	Static addresses	192.168.0.2–192.168.0.127
<net>.128–<net>.254	DHCP-assigned	192.168.0.128–192.168.0.254
<net>.255	Broadcasting	192.168.0.255

Address Use on a NAT Network

Range	Address use	Example
<net>.1	Host machine	192.168.0.1
<net>.2	NAT device	192.168.0.2
<net>.3–<net>.127	Static addresses	192.168.0.3–192.168.0.127
<net>.128–<net>.254	DHCP-assigned	192.168.0.128–192.168.0.254
<net>.255	Broadcasting	192.168.0.255

Avoiding IP Packet Leakage in a Host-Only Network

By design, each host-only network should be confined to the host machine on which it is set up. That is, no packets sent by virtual machines on this network should "leak out" to a physical network attached to the host. Packet leakage can occur only if a machine actively forwards packets. It is possible for the host machine or any virtual machine running on the host-only network to be configured in a way that permits packet leakage.

Windows Hosts

Windows Server 2003, Windows 2000 Server, Windows 2000 Advanced Server and Windows NT systems are capable of forwarding IP packets that are not addressed to them. By default, however, these systems come with IP packet forwarding disabled.

If you find packets leaking out of a host-only network on a Windows NT or Windows 2000 host computer, check to see if forwarding has been enabled on the host machine. If it is enabled, disable it.

On a Windows Server 2003 or Windows 2000 host, go to **Start** > **Programs** > **Administrative Tools** > **Routing and Remote Access**. An icon on the left is labeled with the host name. If a green dot appears over the icon, IP forwarding is turned on. To turn it off, right-click the icon and choose disable **Routing and Remote Access**. A red dot appears, indicating that IP forwarding is disabled.

On a Windows NT host, go to **Start** > **Settings** > **Control Panel** > **Networking**. Choose **TCP/IP**, click **Properties**, then click the **Routing** tab. Clear the check box to disable IP forwarding.

Linux Hosts

If you find packets leaking out of a host-only network on a Linux host computer, check to see if forwarding has mistakenly been enabled on the host machine. If it is enabled, disable it.

For many Linux systems, disable forwarding by writing a 0 (zero) to the special file `/proc/sys/net/ipv4/ip_forward`. As root, enter this command:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

Other Linux systems have a system configuration option that you can set. The method depends on your Linux distribution. You may use a control panel, specify a setting at the time you compile your kernel or possibly enter a specification when you boot your system. Consult your operating system documentation for details on the method to use with your particular distribution.

Using Filtering

If the host computer has multiple network adapters, it may be intentionally configured to do IP forwarding. If that is the case, you do not want to disable forwarding. In that case, to avoid packet leakage you must enable a packet filtering facility and specify that packets from the host-only network should not be sent outside the host computer. Consult your operating system documentation for details on how to configure packet filtering.

Leaks from a Virtual Machine

Virtual machines may leak packets, as well. For example, if you use Dial-Up Networking support in a virtual machine and packet forwarding is enabled, host-only network traffic may leak out through the dial-up connection.

To prevent the leakage, be sure packet forwarding is disabled in your guest operating system.

Changing the MAC Address of a Virtual Machine

When a virtual machine is powered on, GSX Server automatically assigns each of its virtual network adapters a MAC address. MAC stands for media access control. A MAC address is the unique address assigned to each physical network device.

The software guarantees that virtual machines are assigned unique MAC addresses within a given host system. However, the software does not guarantee that a given virtual machine is assigned the same MAC address every time it is powered on. In addition, GSX Server does its best, but cannot guarantee, to automatically assign unique MAC addresses for virtual machines running on multiple host systems.

If you want to guarantee that the same MAC address is assigned to a given virtual machine every time, or if you want to guarantee a unique MAC address for each virtual machine within a networked environment, you can assign the address manually instead of allowing GSX Server to assign it automatically.

To manually assign the same, unique MAC address to any virtual machine, use a text editor to add the following line to its configuration file (the `.vmx` file on a Windows host or `.cfg` file on a Linux host):

```
ethernet0.address = 00:50:56:XX:YY:ZZ
```

where `XX` must be a valid hex number between `00h` and `3Fh`, and `YY` and `ZZ` must be valid hex numbers between `00h` and `FFh`. Because GSX Server virtual machines do not support arbitrary MAC addresses, the above format must be used.

So long as you choose `XX:YY:ZZ` so it is unique among your hard-coded addresses (where `XX` is a valid hex number between `00h` and `3Fh`, and `YY` and `ZZ` are valid hex

numbers between 00h and FFh), conflicts between the automatically assigned MAC addresses and the manually assigned ones should never occur.

Controlling Routing Information for a Host-Only Network on a Linux Host

A host-only network is a full-fledged network. It has a network interface associated with it (VMnet1) that is marked "up" at the time the host operating system is booted. Consequently, routing server processes that operate on the host operating system, such as `routed` and `gated`, automatically discover it and propagate information on how to reach it unless you explicitly configure them not to do so.

If either of these programs is being run only to receive routing information, the easiest solution is to run them with a `-q` option so that they do not supply routing information, only receive it.

If, however, they are running because they are to supply routing information, then you need to configure them so they do not advertise routes to the host-only network.

Unfortunately, the version of `routed` that comes with many distributions of Linux has no support for specifying that an interface should not be advertised. Consult the `routed(8)` manual page for your system in case you have a more contemporary version of the software.

For `gated`, configuration is involved. You need to explicitly exclude the VMnet1 interface from any protocol activity. If you need to run virtual machines on a host-only network on a multihomed system where `gated` is used and have problems doing so, please contact VMware technical support by submitting a support request at *www.vmware.com/requestsupport*.

Other Potential Issues with Host-Only Networking on a Linux Host

The following are common issues you may encounter when you are configuring a host-only network.

DHCPD on the Linux Host Does Not Work after GSX Server Installation

If you were running the DHCP server program `dhcpd` on your machine before installing GSX Server, it probably was configured to respond to DHCP requests from clients on any network interface present on the machine. When host-only networking is configured, an additional network interface, VMnet1, is marked "up" and available for use, and `dhcpd` may notice this.

In such cases, some dhcpd implementations abort if their configuration files do not include a subnet specification for the interface — even if dhcpd is not supposed to respond to messages that arrive through the interface.

The best solution to this problem is to add a line to the dhcpd configuration file of the form:

```
subnet <net>.0 netmask 255.255.255.0 {}
```

<net> is the network number assigned to your host-only network; for example, 192.168.0. This informs dhcpd about the host-only network and tells it explicitly not to respond to any DHCP requests it sees coming from it.

An alternative solution is to explicitly state the set of network interfaces that you want dhcpd to listen to each time you start the program. For example, if your machine has one Ethernet interface, eth0, then each time you start dhcpd, list it on the command line:

```
dhcpd eth0
```

This keeps it from probing for all available network interfaces.

If the above solutions do not work for your DHCP server program, then it likely is old. You can try upgrading to a more current version such the Version 2 DHCP software available from the ISC (*www.isc.org*).

DHCP and Dynamic Domain Name Service (DDNS)

DHCP can be used to hand out IP addresses as well as other information, such as the identity of a host running a name server and the nearest router or gateway. But it does not currently provide a means to dynamically establish a relationship between the IP address it assigns and a client's name (that is, to update a DNS server using DDNS).

This facility is scheduled to be part of the Version 3 DHCP server available from the Internet Software Consortium. When that is available VMware will update GSX Server to use that server.

In the meantime, if you want to use names to communicate with other virtual machines you must either edit the DHCP configuration file for VMnet1 (/etc/vmware/vmnet1.conf) or use IP addresses that are statically bound to a host name. Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. Consult the manual pages dhcpd(8) and dhcpd.conf(8).

Using Samba for File Sharing on a Linux Host

On a Linux host computer, GSX Server can automatically install and configure a Samba server to act as a file server for Microsoft Windows guest operating systems.

You can then use Windows Explorer in the virtual machine to move and copy files between virtual machine and host — or between virtual machines on the same network — just as you would with files on physical computers that share a network connection.

The lightly modified Samba server installed by GSX Server runs over the GSX Server virtual Ethernet, and the Samba traffic between different operating systems is isolated from actual local area networks.

The source code differences for the changes (in `diff` format and based on Samba 2.0.6) are available from VMware. For more information, see *www.vmware.com/download/open_sources.html*.

If you already have Samba configured on your Linux host, the recommended approach is to modify that configuration so it includes the IP subnet used by the GSX Server virtual Ethernet adapter, VMnet1.

You can configure your existing Samba server to work with a host-only network. Note, however, that all the shares you set up in Samba and in the guest operating system normally appear on the bridged network, as well.

If you need to be sure the shares set up in the guest operating system are seen only on the host-only network, you may find it easiest to install and use the Samba server provided with GSX Server.

If you do not need any shares to appear on your bridged network, you can use your existing Samba server and set up the configuration file so it works only on the host-only network.

Samba configurations can be quite complex. This section provides several sample configuration files. If you need to go beyond the issues covered here, see the man page for the `smb.conf` file. To view this page, type one of the following commands in a terminal window:

```
man smb.conf
```

or

```
man 5 smb.conf
```

Pay particular attention to the section on encrypted passwords. If you have enabled clear-text passwords in the guest operating system, be sure that `smb.conf` is set up

to use clear-text passwords. Similarly, if you are using encrypted passwords, you must have the same setting in the guest operating system and in `smb.conf`.

Note: Using Samba printer sharing with virtual machines is not supported. Consult the man pages for guidance on configuring Samba for printing.

Sample smb.conf for Host-Only Networking

The following sample Samba configuration file is for use with host-only networking. This configuration is for the 2.0.6 version of Samba installed by GSX Server. The configuration files are placed in `/etc/vmware/vmnet1/smb` by default.

```
# This is the VMware(TM) Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options
# most of which are not shown in this example
#
# Any line that starts with a ; (semicolon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
#
# Configuration file for Samba 2.0.6 vmware-[sn]mbd operating on
# vmnet1.
#
# This file was generated by the VMware configuration
# program and modified for this document.
#
# If you modify it, it will be backed up the next time you run the
# configuration program.

# Global settings
[global]

# This should be polled at install time from the private subnet created by
# vmware-config.pl
socket address = 192.168.183.1
interfaces = vmnet1
bind interfaces only = yes

workgroup = WORKGROUP
netbios name = HOSTNAME
server string = VMware host-only

security = user
encrypt passwords = yes

# Note: Printers not loaded in this example. Resource definitions commented
# below.
; load printers = yes

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

# VMware extension to use a different shared memory access key on each
# Samba server running on this host
```

```
sysv shm key = /dev/vmnet1

; log file = /etc/vmware/vmnet1/smb/var/log.smb
; log level = 1
; max log size in KB
; max log size = 50

lock directory = /etc/vmware/vmnet1/smb/var/locks

smb passwd file = /etc/vmware/vmnet1/smb/private/smbpasswd

codepage dir = /usr/lib/vmware/smb/codepages

dns proxy = no

# Shared resources

# Home directories
[homes]
comment = Home directories
browseable = no
writable = yes

# Printers
;[printers]
; comment = All printers
; path = /var/lpd
; browseable = no
; guest ok = no
; writable = no
; printable = yes

;[HostFS]
; comment = VMware host filesystem
; path = /
; public = no
; writeable = yes
; printable = no
```

Sample smb.conf for Bridged Networking

The following sample Samba configuration file is for use with bridged networking. This configuration file is based on the 2.0.7 version of Samba and assumes that you are using your existing Samba server, as provided with your host computer's Linux distribution. The configuration file is placed in `/etc` by default.

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options
# most of which are not shown in this example
#
# Any line that starts with a ; (semicolon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command
```

```
# "testparm" to check that you have not many any basic syntactic
# errors.

# Global Settings

[global]

interfaces = eth0

workgroup = WORKGROUP
netbios name = HOSTNAME
server string = Samba Host Box

# Note: Printers not loaded in this example. Resource definitions commented
# below.
; printcap name = lpstat
; load printers = yes
; printing = cups

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

log file = /var/log/samba/log.%m
max log size = 50

security = user
encrypt passwords = yes
smb passwd file = /etc/smbpasswd

dns proxy = no

preserve case = yes
short preserve case = yes
default case = lower
; case sensitive = no

# Shared Resources

[homes]
comment = Home Directories
browseable = yes
writable = yes

;[printers]
; comment = All Printers
; path = /var/spool/samba
; browseable = yes
; guest ok = yes
; writable = no
; printable = yes
; create mode = 0700
; print command = lpr-cups -P %p -o raw %s -r # using client side
; printer drivers.
; print command = lpr-cups -P %p %s # using cups own drivers (use
; generic PostScript on clients).
; lpq command = lpstat -o %p
; lprm command = cancel %p-%j

;[system]
```

```
; comment = System share
; path = /
; valid users = username
; public = no
; browsable = yes
; writable = yes
; printable = no
```

Adding User Names and Passwords to the GSX Server Samba Password File

You must be sure the Samba password file includes entries for all users of the virtual machine who will access the host's file system. The user names and passwords in the Samba password file must be the same as those used for logging on to the guest operating system.

You may add user names and passwords to the GSX Server Samba password file at any time from a terminal window on your Linux host computer.

1. Log on to the root account.
   `su -`
2. Run the GSX Server Samba password command.
   `vmware-smbpasswd vmnet1 -a <username>`
   `<username>` is the user name you want to add. Follow the instructions on the screen.

   Note: `vmware-smbpasswd` is based on the standard Samba password program. If you are familiar with the options used in `smbpasswd`, you may use any of them in `vmware-smbpasswd`.
3. Log out of the root account.
   `exit`

You may receive an error message that says

```
Unknown virtual interface "vmnet1"
```

This indicates your machine is not using the GSX Server Samba server.

If your installation of GSX Server does not include the GSX Server Samba server and you want to set it up, log on to the root account on your host computer (`su -`), then run `vmware-config.pl` from a terminal on the host. The configuration program asks

```
Do you want this script to automatically configure your
system to allow your virtual machines to access the host
file system?
```

Answer Yes.

If You Are Already Running Samba

If you already have Samba running on your Linux host, you should not install the GSX Server Samba server when you are installing GSX Server.

The configuration program prompts you

```
Do you want this script to automatically configure your
system to allow your virtual machines to access the host
file system?
```

Answer No.

Be sure to modify your Samba configuration so it includes the IP subnet used by the GSX Server virtual Ethernet adapter, VMnet1.

To determine what subnet is being used by VMnet1, run

```
/sbin/ifconfig vmnet1
```

You must be sure the Samba password file includes entries for all users of the virtual machine who will access the host's file system. The user names and passwords in the Samba password file must be the same as those used for logging on to the guest operating system.

You may add user names and passwords to the Samba password file at any time from a terminal window on your Linux host computer.

1. Log on to the root account.
   `su -`
2. Run the Samba password command.
   `smbpasswd -a <username>`
   `<username>` is the user name you want to add. Follow the instructions on the screen.
3. Log out of the root account.
   `exit`

Using a Samba Server for Both Bridged and Host-Only Networks

You may use the Samba server of your choice — either the existing Samba server from your host operating system's distribution or the one provided with GSX Server — for both host-only and bridged networking. To do so, you must modify one parameter in the `smb.conf` file. You can define the `interface` parameter so your Samba server serves multiple interfaces. An example of this is:

```
interface = eth0 vmnet1
```

This example tells the Samba server that it is to listen to and use both the `eth0` and `vmnet1` interfaces — the interfaces used by bridged and host-only networking.

Using GSX Server's Samba with an Existing Installation

It may also be possible to run both your existing Samba server and the GSX Server Samba server at the same time. In order to do this, your current Samba server must be version 2.0.6 or higher and must be configured correctly. However, this is not recommended.

To determine the version of your Samba server, run

```
smbd -V
```

If you want to try running both Samba servers at the same time, use this sample `smb.conf` file as a basis for configuring the regular Samba server on your host computer.

Sample smb.conf for Running Two Samba Servers at the Same Time

```
; This file is the recommended smb.conf file for your
; normal Samba server if you want to run it concurrently
; (which we don't advise) with the VMware Samba server.
;
; Your normal samba server should be at least v 2.0.6
;
; Note that you will need to insert specific information
; for your system at several points indicated in the file
; by <text in angle brackets>.
;
; --------------
;
; Larmor samba server configuration
;
; Global settings
[global]
;
; Identity
;
; Allow several Samba servers on the same machine
interfaces = <your real subnet>/<your real netmask>
bind interfaces only = yes
; Workgroup the host belongs to
workgroup = VMware
; SMB name of the host (the hostname by default)
netbios name = <your Windows name>
; Description of the host
server string = Linux running Samba 2.0.6
;
; Access
;
; Allow connections from
; hosts allow = <your real subnet>/<your real netmask>
; Authentication scheme
security = user
encrypt passwords = yes
;
; Options
;
; Automatically load the printer list (from /etc/printcap
```

```
; by default)
load printers = yes
; Gives better performance
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
;
; Files and directories
;
; Max log size in KB
max log size = 1024
; Locks
lock directory = /var/samba
; SMB passwords
smb passwd file = /etc/samba/smbpasswd
;
; Name browsing
;
; Allow the host to participate in master browser
; elections
local master = yes
; Force a local browser election upon startup
; We need that otherwise it takes a long time before the
; windows network is browsable
preferred master = yes
; Do not try to resolve SMB names via DNS
dns proxy = no

; Shared resources
;
; Home directories
[homes]
comment = Home directories
browseable = no
writable = yes
; Printers
;[printers]
; comment = All printers
; path = /var/lpd
; browseable = no
; guest ok = no
; writable = no
; printable = yes
[Slash]
comment = Whole filesystem
path = /
public = no
writeable = yes
printable = no
```

Configuring a Virtual Machine to Switch Network Adapters on a Windows NT Host

You may find it helpful to configure a virtual machine so it can use one network adapter when you are in one location and a different network adapter when you are somewhere else. The most common case involves a laptop computer that is sometimes used with a PC Card (PCMCIA) adapter and sometimes docked in a docking station that has its own network adapter.

The Approach

If you are using bridged networking on a Windows NT 4.0 host, the steps in the next section allow you to configure your virtual machine so it can use both network adapters, with each adapter on a different virtual network interface.

Note: On a Windows 2000 or Windows Server 2003 host, it is more convenient to configure your adapters using the procedure described in Configuring Bridged Networking Options on a Windows Host on page 417.

You need to create two separate GSX Server configuration files (`.vmx` files), both of which point to the same virtual or raw disk. One uses a standard bridged networking setup on the VMnet0 virtual switch. The other uses VMnet2. You use one configuration when you want to connect to a network using the PC Card network adapter and the other when you want to use the docking station's adapter.

Step By Step

1. Follow the usual steps to configure your GSX Server virtual machine with one network adapter in place. (In later steps, these instructions assume that this is the PC Card adapter.) Use bridged networking. Test the setup to be sure the virtual machine can boot and run with that network adapter.
2. After you have tested the initial configuration, shut down your virtual machine and close the console. Switch the setup so the other network adapter is being used. For example, if you first configured the computer while the PC Card adapter was in use, you should now set the computer up in the docking station so its adapter is in use.
3. Open a command prompt.
4. Change to the GSX Server programs folder. If you have installed GSX Server in the default location, the command is
   ```
   cd Program Files\VMware\VMware GSX Server\Programs
   ```
5. Run the following command.
   ```
   vnetconfig -s -ib vmnet2
   ```

6. If you get a dialog box that asks which network adapter to use, choose the adapter that is currently installed (not the one you already configured for bridged networking in step 1).
7. Open the Windows NT Services control panel (**Start** > **Settings** > **Control Panel** > **Services**) and be sure that you now have two services for VMnet Bridge (one for VMnet0 and one for VMnet2).
8. Start the service **VMnet Bridge (for VMnet2)**. If it doesn't start, reboot the system and try to start it again.
9. Open the folder where the files for the virtual machine you are configuring are stored.
10. Copy the `.vmx` file under a different name, so that you have two copies — one to use when you are using the PC Card adapter (referred to here as `pcmcia.vmx`) and one to use when you are using the network adapter in the docking station (referred to here as `nic.vmx`).
11. Launch a GSX Server console, select **Open Existing Virtual Machine**, and open the `.vmx` file for the network adapter you will set up on VMnet2 (`nic.vmx` in our example). You probably need to browse to it.
12. Open the Configuration Editor (**Settings** > **Configuration Editor**) and choose **Network Adapter**.
13. From the drop-down list on the right, choose **Custom (VMnet2)**.
14. Be sure the **Save Configuration Changes** check box is checked, then click **OK** to save your changes and close the Configuration Editor.

Now you are ready.

When you are using the PC Card adapter, launch your virtual machine using `pcmcia.vmx`. When you are using the adapter in the docking station, use `nic.vmx`.

Both `.vmx` files are for the same virtual machine. When you choose one, you are just choosing which network adapter to use.

Note: If you make changes to other aspects of one configuration, remember to make the same changes to the other configuration the next time you open it.

Choosing the Network Driver for Windows Server 2003, Windows XP and Windows 2000 Guest Operating Systems

For Windows Server 2003, Windows XP and Windows 2000 virtual machines on a Windows host, you can select the network driver for your virtual machine's networking connection. The `vlance` driver installs automatically, however, you can choose to install the `vmxnet` driver instead, which provides better networking performance. The difference in networking performance is most noticeable if the virtual machine is connected to a Gigabit Ethernet card.

To install this driver, you must install VMware Tools.

If you change to the `vmxnet` driver, you need to reconfigure any networking settings, for example, proxy server or IP address.

Other guest operating systems use the `vlance` driver only.

This section includes steps for:

- Installing the vmxnet Driver in a New Virtual Machine on page 441
- Installing the vmxnet Driver in an Existing Virtual Machine on page 442
- Installing the vmxnet Driver before Installing VMware Tools on page 443

Installing the vmxnet Driver in a New Virtual Machine

If you are creating a new virtual machine with a Windows Server 2003, Windows XP or Windows 2000 guest operating system, you can choose to install the `vmxnet` networking driver for better networking performance over the default `vlance` networking driver. To install the `vmxnet` driver, complete the following steps.

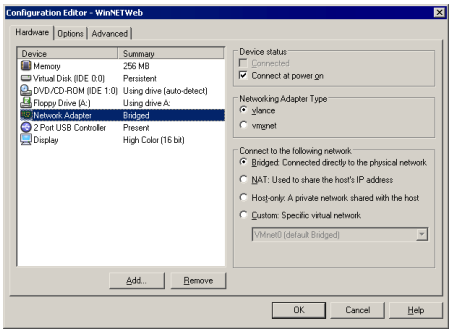
1. Create a new virtual machine. For details, see Creating a New Virtual Machine on page 84.
2. Power on the virtual machine and install the guest operating system.

   To install a Windows Server 2003 guest operating system, see Windows Server 2003 Installation Guidelines on page 257.

   To install a Windows XP guest operating system, see Windows XP Installation Guidelines on page 260.

   To install a Windows 2000 guest operating system, see Windows 2000 Installation Guidelines on page 263.
3. After you install the guest operating system, install VMware Tools in the virtual machine. For information on installing VMware Tools, see Installing VMware Tools in a Windows Virtual Machine on page 113.

4. After you install VMware Tools, shut down the guest operating system and power off the virtual machine. Do not close the console.
5. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
6. On the **Hardware** tab, select the **Network Adapter**.



7. Under **Networking Adapter Type**, select **vmxnet**, then click **OK** to save your changes and close the Configuration Editor.
8. Power on the virtual machine. The guest operating system detects the new virtual hardware. Follow the wizard, then configure the virtual machine's networking options, for example, specify the default gateway, its static IP address and so forth.

Installing the vmxnet Driver in an Existing Virtual Machine

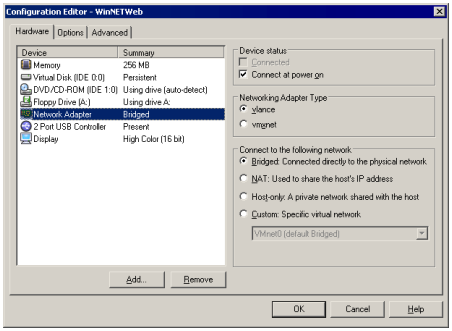
If you have an existing virtual machine with a Windows Server 2003, Windows XP or Windows 2000 guest operating system, you can install the `vmxnet` networking driver for better networking performance over the default `vlance` networking driver. Choosing the `vmxnet` driver causes you to lose any networking settings you made for the `vlance` driver, requiring you to configure networking again.

To install the `vmxnet` driver, complete the following steps.

1. Connect to the virtual machine with a console, start the guest operating system and install VMware Tools. For information on installing VMware Tools, see Installing VMware Tools in a Windows Virtual Machine on page 113.

   Note: Even if you previously installed VMware Tools, you should install it again to make sure you have the version with the `vmxnet` driver.
2. After you install VMware Tools, shut down the guest operating system and power off the virtual machine. Do not close the console.

3. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
4. On the **Hardware** tab, select the **Network Adapter**.



5. Under **Networking Adapter Type**, select **vmxnet**, then click **OK** to save your changes and close the Configuration Editor.
6. Power on the virtual machine. The guest operating system detects the new virtual hardware. Follow the wizard.

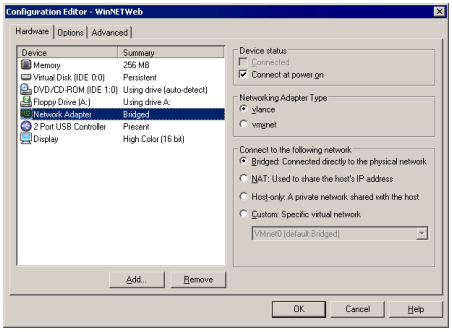
   Since your previous `vlance` networking settings are lost, configure the virtual machine's networking options; for example, specify the default gateway, its static IP address and so forth.

Installing the vmxnet Driver before Installing VMware Tools

You can choose a slightly different installation path to install the `vmxnet` driver. This option may be preferable if you are using scripted installations for your guest operating systems. However, the virtual machine will not have any networking until the latest version of VMware Tools is installed.

1. If you are installing a new virtual machine, complete the following steps; otherwise, go to step 2.
   A. Create a new virtual machine. For details, see Creating a New Virtual Machine on page 84.
   B. Install the guest operating system. To install a Windows Server 2003 guest operating system, see Windows Server 2003 Installation Guidelines on page 257. To install a Windows XP guest operating system, see Windows XP Installation Guidelines on page 260. To install a Windows 2000 guest operating system, see Windows 2000 Installation Guidelines on page 263.
   C. Shut down the guest operating system and power off the virtual machine. Do not close the console.

2. Connect to the virtual machine with a console.
3. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
4. On the **Hardware** tab, select the **Network Adapter**.



5. Under **Networking Adapter Type**, select **vmxnet**, then click **OK** to save your changes and close the Configuration Editor.
6. Power on the virtual machine. The Windows New Hardware Wizard appears as it detects the new network driver. Cancel and close the wizard. At this time, the virtual machine cannot access the network.
7. Install VMware Tools. For information on installing VMware Tools, see Installing VMware Tools in a Windows Virtual Machine on page 113.
8. After you install VMware Tools, configure the virtual machine's networking options, for example, specify the default gateway, its static IP address and so forth.

Configuring Bridged Networking when Using Teamed Network Interface Cards on Your Host

Network adapter teaming (where two or more NICs work together as one and appear as a single, separate device) provides a GSX Server host with a level of network hardware fault tolerance. Should one physical network adapter fail, network traffic for the host and the virtual machines on the host can continue using the remaining network adapters in the team.

If your GSX Server host is configured to use teamed network interface cards, and you use bridged networking with your virtual machines, you need to adjust your network settings. You do this by binding the VMware Bridge Protocol to the teamed NIC, and unbind it from each individual, physical NIC on the host.

Note: VMware has not fully tested bridging of GSX Server virtual machines to host network adapter teams and such configurations are unsupported.

If you want a fully supported alternative for providing network adapter fault tolerance, use automatic bridging instead of using teamed network adapters on the host. See Configuring Bridged Networking Options on a Windows Host on page 417. This feature is available only on Windows hosts. When automatic bridging is enabled, the VMware VMnet0 virtual switch bridges to an automatically chosen host network adapter. Should the host show that the selected network adapter has become unavailable, VMnet0 bridges to remaining host network adapters that have the VMware bridge protocol bound to them.

Known Limitations

1. VMware has not tested network adapter teams with GSX Server on Linux hosts.
2. When using GSX Server on a Windows host with teamed network adapters and bridged networking, the VMware Bridge Protocol must be bound to the teamed network adapter and unbound from the individual physical network adapters. See the steps below.
3. Broadcom-based network adapters cannot be used with Smart Load Balancing (SLB) enabled. GSX Server bridged networking requires that the host network adapters be placed in promiscuous mode. However, Broadcom-based network adapters do not allow promiscuous mode when SLB is enabled. You must use the Generic Trunking option instead. This limitation is documented in the VMware Knowledge Base at *www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=822* and *www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=895*.

4. Receive load balancing should be disabled when using Intel teaming software. VMware has not tested all the modes provided by Intel teaming software.

Windows Host

1. Open the Windows Control Panel. Open Network Connections (Windows Server 2003 host), Network and Dial-up Connections (Windows 2000 host) or Network (Windows NT host).
2. To bind the VMware Bridge Protocol to the teamed NIC, do the following:

   On a Windows Server 2003 or Windows 2000 host, right-click the teamed NIC device and choose **Properties**. Check **VMware Bridge Protocol**, then click **OK** to close the property sheet.

   On a Windows NT host, click the **Bindings** tab. In the **Show Bindings for** list, select **all protocols**. Expand the **VMware Bridge Protocol** tree, select the teamed NIC and click **Enable**. Click **OK** to close the Network dialog box.
3. To unbind the VMware Bridge Protocol from each physical NIC that is being used for bridged networking, do the following:

   On a Windows Server 2003 or Windows 2000 host, right-click the NIC device and choose **Properties**. Uncheck **VMware Bridge Protocol**, then click **OK** to close the property sheet.

   On a Windows NT host, click the **Bindings** tab. In the **Show Bindings for** list, select **all protocols**. Expand the **VMware Bridge Protocol** tree, select the physical NIC and click **Disable**. Click **OK** to close the Network dialog box.

Setting Up a Second Bridged Network Interface on a Linux Host

If you have two Ethernet adapters installed on your host computer, connected to two different networks, you may want your virtual machines on that host computer to bridge to both Ethernet adapters so the virtual machines can access either or both physical networks.

When you install GSX Server on a host computer with multiple Ethernet adapters, you have the option of configuring more than one bridged network. You can also configure additional bridged networks at any time by running the `vmware-config.pl` configuration program again.

1. On the host computer, become root (`su -`) and run the GSX Server configuration program.
   ```
   vmware-config.pl
   ```
2. If you have more than one physical Ethernet adapter, one of the prompts you see is similar to this:

```
The following bridged networks have been defined:
. vmnet0 is bridged to eth0
Do you wish to configure another bridged network? (yes/no)
[no]
```

Enter `yes`.

3. If you have additional physical Ethernet adapters not yet connected to a bridged network, the prompt is repeated, showing information about all currently configured bridged networks.
4. When you have set up all the bridged networks you want, enter `no`.

Setting Up Two Separate Host-Only Networks

For some configurations, you may need to set up more than one host-only network on the same host computer.

You may, for example, want to have two virtual machines connected to one host-only network, and at the same time have other virtual machines connected to another host-only network so the network traffic on each network is isolated.

Or you may want to test routing between two virtual networks. Or test a virtual machine with multiple network interface cards — without using any physical Ethernet adapters.

On Windows hosts, the first host-only network is set up automatically when you install GSX Server.

On Linux hosts, the first host-only network was set up when you ran the `vmware-config.pl` program after you installed GSX Server, provided you agreed to install host-only networking. If you did not agree to use host-only networking, you need to run the program again to set up host-only networking.

To set up the second host-only network, follow the steps outlined below for your host operating system.

Setting Up the Second Host-Only Interface – Windows Server 2003 Host

1. Start the Add Hardware Wizard.

   Start > Control Panel > Add Hardware

   Note: You must have sufficient privileges to do this.
2. Click **Next**.
3. When prompted, select **Yes, I have already connected the hardware**.
4. On the screen that lets you select the hardware, select **Add a new hardware device**, then click **Next**.

5. Select **Install the hardware that I manually select from a list (Advanced)**.
6. Select **Network Adapter**.
7. Select **VMware, Inc.** as the manufacturer.
8. Select the host-only adapter for the appropriate VMnet.
9. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
10. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Windows 2000 Host

1. Open the Control Panel (**Start** > **Settings** > **Control Panel**).
2. Start the Add/Remove Hardware Wizard from the Control Panel.

   Note: You must have sufficient privileges to do this.
3. Click **Next** to continue past the Welcome screen.
4. Select **Add/Troubleshoot a Device** and click **Next**.
5. Wait while Windows searches for new Plug and Play devices, then select **Add a New Device** from the Choose a Hardware Device screen and click **Next**.
6. Select **No, I want to select the hardware from a list** and click **Next**.
7. Select **Network Adapters** from the list and click **Next**.
8. Select **VMware, Inc.** from the manufacturers list on the Select Network Adapter screen to get the list of available host-only network adapters. Select **VMware Virtual Ethernet Adapter (for VMnet2)** and click **Next**.
9. Click **Next** in the Start Hardware Installation screen.
10. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
11. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Windows NT Host

Follow these steps to set up the second host-only interface on Windows NT.

1. Open a command prompt window. Change to the GSX Server programs folder. If you accepted the default path, use this command:

   ```
   cd C:\Program Files\VMware\VMware GSX Server
   ```
2. Run the following command:

   ```
   vnetconfig -ih vmnet2
   ```

Setting Up the Second Host-Only Interface – Linux Host

1. As root (`su -`), run the GSX Server configuration program.

   ```
   /usr/bin/vmware-config.pl
   ```

2. Use the wizard to modify your configuration. After asking about a NAT network, the program asks:

   ```
   Do you want to be able to use host-only networking in your
   virtual machines?
   ```

   Answer Yes.

   The wizard reports on host-only networks that you have already set up on the host or, if none is present, configures the first host-only network.

3. The wizard asks:

   ```
   Do you wish to configure another host-only network?
   ```

   Answer Yes.

   Repeat this step until you have as many host-only networks as you want. Then answer No.

4. Complete the wizard. When it is finished, it restarts all services used by GSX Server.

5. Run `ifconfig`. You should see at least four network interfaces — `eth0`, `lo`, `vmnet1` and `vmnet2`. If the VMnet interfaces do not show up immediately, wait for a minute, then run the command again. These four interfaces should have different IP address on separate subnets.

Configuring the Virtual Machines

Now you have two host-only interfaces (VMnet1 and VMnet2). You are ready to configure your virtual machines for one of the following scenarios:

1. The virtual machine is configured with one virtual Ethernet adapter, and that virtual adapter is connected to the default host-only interface (VMnet 1).
2. The virtual machine is configured with one virtual Ethernet adapter, and that virtual adapter is connected to the newly created host-only interface (VMnet2).
3. The virtual machine is configured with two virtual Ethernet adapters. One virtual adapter is connected to the default host-only interface (VMnet1) and the other virtual adapter is connected to the newly created host-only interface (VMnet2).

Scenario 1 – Connect to the Default Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch a console and open the virtual machine.
3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).

   Windows host: Select **Network Adapter**, then select **Host-only (VMnet1)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

   Linux host: Click the + sign to expand the **Ethernet Adapters** list and select the first adapter. From the **Connection Type** drop-down list on the right, select **Host-only**.

   If the list of devices indicates the adapter is not installed, click **Install**.

Scenario 2 – Connect to the Newly Created Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (Windows hosts) or Configuration Wizard (Linux hosts) or use an existing virtual machine.
2. Launch a console and open the virtual machine.
3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).

   Windows host: Select **Network Adapter**, then select **Custom (VMnet2)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

   Linux host: Click the + sign to expand the **Ethernet Adapters** list and select the first adapter. From the **Connection Type** drop-down list on the right, select **Custom**. In the **VMnet** field, type `/dev/vmnet2`.

   If the list of devices indicates the adapter is not installed, click **Install**.

Scenario 3 – Connect to Two Host-Only Interfaces

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch a console and open the virtual machine.

3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).

   Windows host: Select the first network adapter in the list of devices, then select **Host-only (VMnet1)** from the drop-down list on the right. Select the second network adapter in the list of devices, then select **Custom (VMnet2)** from the drop-down list on the right.

   If you need to add one or more network adapters, click **Add**, then use the Add Hardware Wizard to add an adapter.

   Linux host: Click the **+** sign to expand the **Ethernet Adapters** list and select the first adapter. From the **Connection Type** drop-down list on the right, select **Host-only**.

   If the list of devices indicates the adapter is not installed, click **Install**.

   Select the second adapter and, from the **Connection Type** drop-down list on the right, select **Custom**. In the **VMnet** field, type `/dev/vmnet2`.

   If the list of devices indicates the adapter is not installed, click **Install**.

At this point you can power on the virtual machine and install your guest operating system. In scenarios 1 and 2 you see one AMD PCNet Family Adapter. In scenario 3 you see two AMD PCNet Family Adapters within the guest. Configure the Ethernet adapters as you would physical adapters on a physical computer, giving each an IP address on the appropriate VMnet subnet.

On Windows hosts, you can open a command prompt and run `ipconfig /all` to see what IP addresses each host-only network is using.

On Linux hosts, you can open a terminal and run `ifconfig` to see what IP addresses each host-only network is using.

Routing between Two Host-Only Networks

If you are setting up a complex test network using virtual machines, you may want to have two independent host-only networks with a router between them.

There are two basic approaches. In one, the router software runs on the host computer. In the other, the router software runs in its own virtual machine. In both cases, you need two host-only interfaces.

The examples described here outline the simplest case, with one virtual machine on each of the host-only networks. For more complex configurations, you can add more virtual machines and host-only networks as appropriate.

Setting Up the First Host-Only Interface

On Windows hosts, the first host-only network is set up automatically when you install GSX Server.

On Linux hosts, the first host-only network was set up when you ran the `vmware-config.pl` program after you installed GSX Server, provided you agreed to install host-only networking. If you did not agree to use host-only networking, you need to run the program again to set up host-only networking.

Setting Up the Second Host-Only Interface – Windows Server 2003 Host

1. Start the Add Hardware Wizard.

   Start > Control Panel > Add Hardware

   Note: You must have sufficient privileges to do this.
2. Click **Next**.
3. When prompted, select **Yes, I have already connected the hardware**.
4. On the screen that lets you select the hardware, select **Add a new hardware device**, then click **Next**.
5. Select **Install the hardware that I manually select from a list (Advanced)**.
6. Select **Network Adapter**.
7. Select **VMware, Inc.** as the manufacturer.
8. Select the host-only adapter for the appropriate VMnet.
9. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
10. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Windows 2000 Host

1. Open the Control Panel (**Start** > **Settings** > **Control Panel**).
2. Start the Add/Remove Hardware Wizard from the Control Panel.

   Note: You must have sufficient privileges to do this.
3. Click **Next** to continue past the Welcome screen.
4. Select **Add/Troubleshoot a Device** and click **Next**.
5. Wait while Windows searches for new Plug and Play devices, then select **Add a New Device** from the Choose a Hardware Device screen and click **Next**.
6. Select **No, I want to select the hardware from a list** and click **Next**.
7. Select **Network Adapters** from the list and click **Next**.
8. Select **VMware, Inc.** from the manufacturers list on the Select Network Adapter screen to get the list of available host-only network adapters, then select **VMware Virtual Ethernet Adapter (for VMnet2)** and click **Next**.
9. Click **Next** in the Start Hardware Installation screen.
10. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
11. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Windows NT Host

Follow these steps to set up the second host-only interface on Windows NT.

1. Open a command prompt window. Change to the GSX Server programs folder. If you accepted the default path, use this command:
   ```
   cd C:\Program Files\VMware\VMware GSX Server
   ```
2. Run the following command:
   ```
   vnetconfig -ih vmnet2
   ```

This creates a second host-only adapter, which can be configured from the Network control panel.

Setting Up the Second Host-Only Interface – Linux Host

1. As root (`su -`), run the GSX Server configuration program.
   ```
   /usr/bin/vmware-config.pl
   ```
2. Use the wizard to modify your configuration. When the program asks:
   ```
   Do you want to be able to use host-only networking in
   your virtual machines?
   ```
   Answer Yes.

The wizard reports on host-only networks that you have already set up on the host or, if none is present, configures the first host-only network.

3. The wizard asks:
   `Do you wish to configure another host-only network?`
   Answer Yes.
   Repeat this step until you have as many host-only networks as you want. Then answer No.
4. Complete the wizard. When it is finished, it restarts all services used by GSX Server.
5. Run `ifconfig`. You should see at least four network interfaces — `eth0`, `lo`, `vmnet1` and `vmnet2`. If the VMnet interfaces do not show up immediately, wait for a minute, then run the command again. These four interfaces should have different IP address on separate subnets.

Setting Up the Virtual Machines

Now you have two host-only network adapters on the host computer. Each is connected to its own virtual switch (VMnet1 and VMnet2). You are ready to create and configure your virtual machines and connect them to the appropriate virtual switches.

Virtual Machine 1 – Connected to the Default Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch a console and open the virtual machine.
3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).
   Windows host: Select **Network Adapter** and select **Host-only (VMnet1)** from the drop-down list on the right.
   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.
   Linux host: Click the + sign to expand the **Ethernet Adapters** list and select the first adapter. From the **Connection Type** drop-down list on the right, select **Host-only**.
   If the list of devices indicates the adapter is not installed, click **Install**.

Virtual Machine 2 – Connected to the Newly Created Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch a console and open the virtual machine.
3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).

   Windows host: Select **Network Adapter** and select **Custom (VMnet2)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

   Linux host: Click the + sign to expand the **Ethernet Adapters** list and select the first adapter. From the **Connection Type** drop-down list on the right, select **Custom**. In the **VMnet** field, type `/dev/vmnet2`.

   If the list of devices indicates the adapter is not installed, click **Install**.

If you plan to run the router software on your host computer, you can skip the next section.

Virtual Machine 3 – Connected to Both Host-Only Interfaces

If you plan to run the router software on a virtual machine, set up a third virtual machine for that purpose.

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch a console and open the virtual machine.
3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).

   Windows host: Select the first network adapter in the list of devices and select **Host-only (VMnet1)** from the drop-down list on the right. Select the second network adapter in the list of devices, then select **Custom (VMnet2)** from the drop-down list on the right.

   If you need to add one or more network adapters, click **Add**, then use the Add Hardware Wizard to add an adapter.

Linux host: Click the + sign to expand the **Ethernet Adapters** list and select the first adapter. From the **Connection Type** drop-down list on the right, select **Host-only**.

If the list of devices indicates the adapter is not installed, click **Install**.

Select the second adapter, then from the **Connection Type** drop-down list on the right, select **Custom**. In the **VMnet** field, type `/dev/vmnet2`.

If the list of devices indicates the adapter is not installed, click **Install**.

Now you need to configure the networking components on the host and in the virtual machines. The recommended approach uses static IP addresses for all the virtual machines.

1. Stop the VMnet DHCP server service.

   Windows host: In the Services control panel, find VMware DHCP Server and be sure it is stopped.

   Linux host: Stop the `vmnet-dhcpd` service.

   ```
   killall -TERM vmnet-dhcpd
   ```

2. Install guest operating systems in each of the virtual machines.
3. Install the router software — on the host computer or in the third virtual machine, depending on the approach you are using.
4. Configure networking in the first two virtual machines to use addresses on the appropriate host-only network.

   On Windows hosts, you can open a command prompt and run `ipconfig /all` to see what IP addresses each host-only network is using.

   On Linux hosts, you can open a terminal and run `ifconfig` to see what IP addresses each host-only network is using.

5. If you are running the router on the host computer, assign default router addresses based on the addresses of the host-only adapters on the host computer. In the first virtual machine's networking configuration, the default router address should be the IP address for the host-only adapter connected to VMnet1. In the second virtual machine's networking configuration, the default router address should be the IP address for the host-only adapter connected to VMnet2.

   If you are running the router software on the third virtual machine, set the default router addresses in the first two virtual machines based on those used by the third virtual machine. In the first virtual machine's networking configuration,

the default router address should be the IP address for the third virtual machine's Ethernet adapter connected to VMnet1. In the second virtual machine's networking configuration, the default router address should be the IP address for the third virtual machine's Ethernet adapter connected to VMnet2.

At this point you should be able to ping the router machine from virtual machines one and two. And if the router software is set up correctly, you should be able to communicate between the first and second virtual machines.

Using Virtual Ethernet Adapters in Promiscuous Mode on a Linux Host

GSX Server does not allow the virtual Ethernet adapter to go into promiscuous mode unless the user running GSX Server has permission to make that setting. This follows the standard Linux practice that only root can put a network interface into promiscuous mode.

When you install and configure GSX Server, you must run the installation as root. GSX Server creates the VMnet devices with root ownership and root group ownership, which means that only root has read/write permissions to the devices.

To set the virtual machine's Ethernet adapter to promiscuous mode, you must launch GSX Server as root because you must have read/write access to the VMnet device. For example, if you are using bridged networking, you must have access to `/dev/vmnet0`.

To grant selected other users read/write access to the VMnet device, you can create a new group, add the appropriate users to the group and grant that group read/write access to the appropriate device. You must make these changes on the host operating system as root (`su -`). For example, you can enter the following commands:

```
chgrp <newgroup> /dev/vmnet0
chmod g+rw /dev/vmnet0
```

`<newgroup>` is the group that should have the ability to set `vmnet0` to promiscuous mode.

If you want all users to be able to set the virtual Ethernet adapter (`/dev/vmnet0` in our example) to promiscuous mode, you can simply run the following command on the host operating system as root.

```
chmod a+rw /dev/vmnet0
```

Understanding NAT

Network address translation (NAT) provides a simple way for virtual machines to use most client applications over almost any type of network connection available to the host. The only requirement is that the network connection must support TCP/IP.

NAT is useful when you have a limited supply of IP addresses or are connected to the network through a non-Ethernet network adapter. NAT works by translating addresses of virtual machines in a private VMnet network to that of the host machine. When a virtual machine sends a request to access a network resource, it appears to the network resource as if the request came from the host machine.

NAT uses the host's own network resources to connect to the external network. Thus, any TCP/IP network resource to which the host has access should be available through the NAT connection.

The chief advantage of NAT is that it provides a transparent, easy to configure way for virtual machines to gain access to network resources.

Using NAT in GSX Server

The NAT device is connected to the VMnet8 virtual switch. Virtual machines connected to the NAT network also use the VMnet8 virtual switch.

The NAT device waits for packets coming from virtual machines on the VMnet8 virtual network. When a packet arrives, the NAT device translates the address of the virtual machine to that of the host before forwarding the packet to the external network. When data arrives from the external network for the virtual machine on the private network, the NAT device receives the data, replaces the network address with that of the virtual machine and forwards the data to the virtual machine on the virtual network. This translation occurs automatically and requires minimal configuration on the guest and the host.

The Host Computer and the NAT Network

The host computer has an adapter on the NAT network (identical to the host-only adapter on the host-only network). This adapter allows the host and the virtual machines to communicate with each other for such purposes as file sharing. The NAT never forwards traffic from the host adapter.

DHCP on the NAT Network

In order to make networking configuration easy, a DHCP server is automatically installed when you install GSX Server. Virtual machines running on the network with the NAT device can dynamically obtain their IP addresses by sending out a DHCP request. The DHCP server on the NAT network, which is also used in host-only networking configurations, dynamically allocates IP addresses in the range of <net>.128 through <net>.254, where <net> is the network number assigned to your NAT network. GSX Server always uses a Class C address for NAT networks. IP addresses <net>.3 through <net>.127 can be used for static IP addresses. IP address <net>.1 is reserved for the host-only adapter (VMnet1); <net>.2 is reserved for the NAT device (VMnet8). Thus, with NAT, 2 IP addresses are in use on the host.

In addition to the IP address, the DHCP server on the NAT network also sends out additional configuration information that enables the virtual machine to operate automatically. This information includes the default gateway and the DNS server. In the DHCP response, the NAT device instructs the virtual machine to use the IP address <net>.2 as the default gateway and DNS server. This causes all IP packets destined for the external network and DNS requests to be forwarded to the NAT device.

DNS on the NAT Network

The NAT device acts as a DNS server for the virtual machines on the NAT network. Actually, the NAT device is a DNS proxy and merely forwards DNS requests from the virtual machines to a DNS server that is known by the host. Responses come back to the NAT device, which then forwards them to the virtual machines.

If they get their configuration information from DHCP, the virtual machines on the NAT network automatically use the NAT device as the DNS server. However, the virtual machines can be statically configured to use another DNS server.

The virtual machines in the private NAT network are not, themselves, accessible via DNS. If you want the virtual machines running on the NAT network to access each other by DNS names, you must set up a private DNS server connected to the NAT network.

External Access from the NAT Network

In general, any protocol using TCP or UDP can be used automatically by a virtual machine on the NAT network so long as the virtual machine initiates the network connection. This is true for most client applications such as Web browsing, Telnet, passive-mode FTP and downloading streaming video. Additional protocol support has been built into the NAT device to allow FTP and ICMP echo (ping) to work completely transparently through the NAT.

On the external network to which the host is connected, any virtual machine on the NAT network appears to be the host itself, because its network traffic uses the host's IP address. It is able to send and receive data using TCP/IP to any machine that is accessible from the host.

Before any such communication can occur, the NAT device must set up a mapping between the virtual machine's address on the private NAT network and the host's network address on the external network.

When a virtual machine initiates a network connection with another network resource, this mapping is created automatically. The operation is perfectly transparent to the user of the virtual machine on the NAT network. No additional work needs to be done to let the virtual machine access the external network.

The same cannot be said for network connections that are initiated from the external network to a virtual machine on the NAT network.

When a machine on the external network attempts to initiate a connection with a virtual machine on the NAT network, it cannot reach it because the NAT device does not forward the request. Network connections that are initiated from outside the NAT network are not transparent.

However, it is possible to manually configure port forwarding on the NAT device so network traffic destined for a certain port can still be automatically forwarded to a virtual machine on the NAT network. For details, see Advanced NAT Configuration on page 461.

File sharing of the type used by Windows operating systems and Samba is possible among computers on the NAT network — including virtual machines and the host computer. If you are using WINS servers on your network, a virtual machine using NAT networking can access shares on the host known by the WINS server as long as they are in the same workgroup or domain.

Advanced NAT Configuration

Use the NAT configuration file on the host to configure the NAT device.

On Windows, this file is `vmnetnat.conf`. It is located in the host operating system's system folder (normally `C:\WINNT\system32`).

On Linux, this file is `/etc/vmware/vmnet8/nat/nat.conf`.

The configuration file is divided into sections. Each section configures a part of the NAT device. Text surrounded by square brackets — such as `[host]` — marks the beginning of a section. In each section is a configuration parameter that can be set. The configuration parameters take the form `ip = 192.168.27.1/24`.

For an example of a NAT configuration file, see Sample Windows vmnetnat.conf File on page 466. The configuration file variables are described below.

The [host] Section

`ip`
The IP address that the NAT device should use. It can optionally be followed by a slash and the number of bits in the subnet.

`netmask`
The subnet mask to use for the NAT. DHCP addresses are allocated from this range of addresses.

`configport`
A port that can be used to access status information about the NAT.

`device`
The VMnet device to use. Windows devices are of the form `VMnet<x>` where `<x>` is the number of the VMnet. Linux devices are of the form `/dev/vmnet<x>`. VMnet8 is the default NAT device.

`activeFTP`
Flag to indicate if active FTP is to be allowed. Active FTP allows incoming connections to be opened by the remote FTP server. Turning this off means that only passive mode FTP works. Set to `0` to turn it off.

The [udp] Section

`timeout`
Number of seconds to keep the UDP mapping for the NAT.

The [dns] Section

This section is for Windows hosts only. Linux does not use this section.

`policy`
Policy to use for DNS forwarding. Accepted values include `order`, `rotate` and `burst`.

- `order` — send one DNS request at a time in order of the name servers
- `rotate` — send one DNS request at a time and rotate through the DNS servers
- `burst` — send to three servers and wait for the first one to respond

`timeout`
Time in seconds before retrying a DNS request.

`retries`
Number of retries before the NAT device gives up on a DNS request.

`autodetect`
Flag to indicate if the NAT should automatically detect the DNS servers available to the host.

`nameserver1`
IP address of a DNS server to use.

`nameserver2`
IP address of a DNS server to use.

`nameserver3`
IP address of a DNS server to use.

If autodetect is on and some name servers are specified, the DNS servers specified in `nameserver1`, `nameserver2` and `nameserver3` are added before the list of detected DNS servers.

The [netbios] Section

This section applies to Windows hosts only. Linux does not use this section.

`nbnsTimeout = 2`
Timeout for NBNS queries.

`nbnsRetries = 3`
Number of retries for each NBNS query.

`nbdsTimeout = 3`
Timeout for NBDS queries.

The [incomingtcp] Section

This section is used to configure TCP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section.

```
8887 = 192.168.27.128:21
```

This creates a mapping from port 8887 on the host to the IP address 192.168.27.128 and port 21. When this is set and an external machine connects to the host at port 8887, the network packets are automatically forwarded to port 21 (the standard port for FTP) on the virtual machine with IP address 192.168.27.128.

The [incomingudp] Section

This section is used to configure UDP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section. It illustrates a way to forward X server traffic from the host port 6000 to the virtual machine's port 6001.

```
6000 = 192.168.27.128:6001
```

This creates a mapping from port 6000 on the host to the IP address 192.168.27.128 and port 6001. When this is set and an external machine connects to the host at port 6000, the network packets are automatically forwarded to port 6001 on the virtual machine with IP address 192.168.27.128.

Considerations for Using NAT

Because NAT requires that every packet sent and received from virtual machines is in the NAT network, there is an unavoidable performance penalty. Our experiments show that the penalty is minor for dial-up and DSL connections and performance is adequate for most GSX Server uses.

NAT is not perfectly transparent. It does not normally allow connections to be initiated from outside the network, although you can set up server connections by manually configuring the NAT device. The practical result is that some TCP and UDP protocols that require a connection be initiated from the server machine — some peer to peer applications, for example — do not work automatically, and some may not work at all.

A standard NAT configuration provides basic-level firewall protection because the NAT device can initiate connections from the private NAT network, but devices on the external network cannot normally initiate connections to the private NAT network.

Using NAT with NetLogon (Windows Hosts and Virtual Machines Only)

When using NAT networking in a virtual machine with a Windows guest operating system running on a Windows host, you can utilize NetLogon to log on to a Windows domain from the virtual machine. This allows you to access file shares known by the WINS server in the domain.

To use NetLogon, you need to know how WINS servers and Windows domain controllers work. This section only explains how to set up the virtual machine to use NetLogon. The setup process is similar to the way you would set up a physical computer on one LAN that is using a domain controller on another LAN.

In order to log on to a Windows domain outside the virtual NAT network, the virtual machine needs access to a WINS server for that domain. There are two ways the virtual machine can connect to the WINS server. You can connect to the WINS server provided by the DHCP server used on the NAT network, provided that the WINS server is already set up on the host. If you want to connect from the virtual machine to a WINS server not set up on the host, you can manually enter the IP address of the WINS server.

Using NAT to Connect to an Existing WINS Server Already Set Up on the Host

In order to use this method, a WINS server in the same workgroup or domain must be set up on the host. These steps use Windows 2000, Windows XP or Windows Server 2003 as a guide. The process is similar for Windows NT, Windows Me and Windows 9x guests.

1. In the virtual machine, right-click **My Network Places** and select **Properties**.
2. In the Network Connections window, right-click the virtual network adapter and select **Properties**.
3. In the Properties dialog, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog, click **Advanced**.
5. Click the **WINS** tab, then under **NetBIOS setting**, select **Use NetBIOS setting from DHCP Server**.
6. Click **OK** twice, then click **Close**.

Manually Entering the IP Address of a WINS Server

Use this method to connect to a WINS server in the same workgroup or domain that is not already set up on the host.

1. In the virtual machine, right-click **My Network Places** and select **Properties**.
2. In the Network Connections window, right-click the virtual network adapter and select **Properties**.
3. In the Properties dialog, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog, click **Advanced**.
5. Click the **WINS** tab, then click **Add**.
6. In the TCP/IP WINS Server dialog box, enter the IP address for the WINS server in the **WINS server** field, then click **OK**. The IP address of the WINS server appears in the **WINS addresses** list on the **WINS** tab.

   Repeat steps 5 and 6 for each WINS server you want to connect to from this virtual machine.
7. Click **OK** twice, then click **Close**.

Now that the virtual machine has an IP address for a WINS server, you use NetLogon in the virtual machine to log on to a domain and access shares in that domain.

For example, if the WINS server covers a domain with a domain controller it is possible to access that domain controller from the virtual machine and add the virtual machine to the domain. You need to know the Administrator's user ID and password of the domain controller.

Note: You can access shares of virtual machines that are only on the same NAT network or are bridged on the same domain.

Sample Windows vmnetnat.conf File

```
# Windows NAT configuration file

[host]
# NAT gateway address
ip = 192.168.237.2/24
hostMAC = 00:50:56:C0:00:08

# enable configuration; disabled by default for security reasons
#configport = 33445

# VMnet device if not specified on command line
device = VMnet8

# Allow PORT/EPRT FTP commands (they need incoming TCP stream...)
activeFTP = 1

# Allows the source to have any OUI. Turn this one if you change the OUI
# in the MAC address of your virtual machines.
#allowAnyOUI = 1

[udp]
# Timeout in seconds, 0 = no timeout, default = 60; real value might
# be up to 100% longer
timeout = 30

[dns]
# This section applies only to Windows.
#
# Policy to use for DNS forwarding. Accepted values include order,
# rotate, burst.
#
# order: send one DNS request at a time in order of the name servers
# rotate: send one DNS request at a time, rotate through the DNS servers
# burst: send to three servers and wait for the first one to respond
policy = order;

# Timeout in seconds before retrying DNS request.
timeout = 2

# Retries before giving up on DNS request
retries = 3

# Automatically detect the DNS servers (not supported in Windows NT)
autodetect = 1
```

```
# List of DNS servers to use. Up to three may be specified
#nameserver1 = 208.23.14.2
#nameserver2 = 63.93.12.3
#nameserver3 = 208.23.14.4

[netbios]
# This section applies only to Windows.

# Timeout for NBNS queries.
nbnsTimeout = 2

# Number of retries for each NBNS query.
nbnsRetries = 3

# Timeout for NBDS queries.
nbdsTimeout = 3

[incomingtcp]
# Use these with care - anyone can enter into your virtual machine through
# these...

# FTP (both active and passive FTP is always enabled)
#      ftp localhost 8887
#8887 = 192.168.27.128:21

# WEB (make sure that if you are using named webhosting, names point to
#     your host, not to guest... And if you are forwarding port other
#     than 80 make sure that your server copes with mismatched port
#     number in Host: header)
#      lynx http://localhost:8888
#8888 = 192.168.27.128:80

# SSH
#      ssh -p 8889 root@localhost
#8889 = 192.168.27.128:22

[incomingudp]
# UDP port forwarding example
#6000 = 192.168.27.128:6001
```

13

Video and Sound

Configuring Video and Sound in VMware GSX Server

The following sections provide information on configuring the video display and sound for VMware GSX Server.

- Setting Screen Colors in a Virtual Machine on page 471
  - Changing Screen Colors on the Host on page 471
  - Changing Screen Colors in the Guest on page 472
- Changing XFree86 Video Resolutions on a Linux Host on page 473
  - Configuration on page 473
  - Possible Issues on page 473
- Configuring Sound in GSX Server on page 475
  - Setting Up a Virtual Sound Card on a Windows Host on page 475
  - Setting Up a Virtual Sound Card on a Linux Host on page 476
  - Setting Up Sound in the Guest Operating System on page 476
  - Improving Sound Performance on page 479

Setting Screen Colors in a Virtual Machine

The number of screen colors available inside a virtual machine depends on the screen color setting of the host computer.

On a Windows host, all guests support

- The number of colors set on the host at the time the guest operating system was started
- 256 colors (8-bit mode)
- In some cases, 16 colors (4-bit mode)

On a Linux host, all guests support

- The same number of colors as set on the host

If you run a virtual machine set for a greater number of colors than your host computer is using, you can encounter various problems. In some cases, for example, the colors in the guest will not be correct. In others, the virtual machine will not be able to use a graphical interface.

In such a case, you can either increase the number of colors available on the host or decrease the number of colors used in the guest.

Changing Screen Colors on the Host

If you choose to change the color settings on your host computer, you should first shut down the guest operating system, power off the virtual machine and close the console.

Follow standard procedures for changing the color settings on your host computer, then restart the console and the virtual machine.

Changing Screen Colors in the Guest

If you choose to change the color settings in the guest operating system, the approach depends on the combination of host and guest you are using.

Windows Guests

Follow the normal process for changing screen colors in your guest operating system. In a Windows guest running on a Windows host, the Display Properties control panel offers only settings that are supported, as described above.

A Windows guest running on a Linux host adjusts automatically to the number of colors supported on the host computer. You do not need to take any special steps.

Linux Guests

In a Linux guest, you must change the color depth before you start the X server.

Changing XFree86 Video Resolutions on a Linux Host

You can configure GSX Server on a Linux host to change the full screen display resolution to better match the resolution set in the guest operating system. On a Windows host, this is done by default and you do not need to change any configuration settings.

GSX Server uses the VidMode extension from the XFree86 Project to match the host resolution to the one requested by the guest running in the virtual machine.

Configuration

The option **Find best resolution in full screen mode** is on by default. When on, this option allows GSX Server to locate the best resolution for your host operating system, thus minimizing or eliminating the black border that earlier versions of GSX Server displayed when the guest operating system was in full screen mode.

You can change the default for **Find best resolution in full screen mode** by going to the **Misc** panel in the Configuration Editor (**Settings** > **Configuration Editor**).

Possible Issues

In a few cases, the **Find best resolution …** option may not give the best results.

X Server Configuration

The VidMode extension can choose only resolutions that are already configured in the `XF86Config` file on your host. A sample configuration for a given color depth could look like this:

```
Subsection "Display"
Depth 16
Modes "1280x1024" "1024x768" "800x600"
ViewPort 0 0
EndSubsection
```

In this case, GSX Server is able to match a virtual machine running at 1280×1024, 1024×768 or 800×600 but not at 640×480 or 1152×900. If a virtual machine runs at a resolution that does not match a mode listed in the XFree86 configuration, then GSX Server chooses the closest larger mode or else simply does not switch modes at all.

It is possible to have bad modes configured in the `XF86Config` file on your host. If your XFree86 configuration was automatically generated, or if you never tested all modes with your current monitor and video card, it is possible that some enabled

modes do not work with your monitor. However, the VidMode code in GSX Server has no way of knowing this and a virtual machine that tries to use a resolution with a bad mode line can cause your display to fail to display correctly.

If this happens, immediately leave full screen mode by pressing Ctrl-Alt, then either disable the mode switching code in GSX Server or fix your XFree86 configuration and restart X. However, if the only problem is that the image is off center or is not quite the right size on the monitor, you can usually correct it using the controls on your monitor. Note that most modern monitors are capable of storing separate settings for each resolution, so changing the settings for a new mode should not impair the settings for the host resolution.

Mouse Movement

The mouse may completely fail to move while in a full screen mode virtual machine.

In XFree86 version 3.3.3.0, the DirectMouse interface does not operate properly. The interface works correctly in previous and subsequent releases of XFree86. XFree86 version 3.3.3.0 was not included in any mainstream Linux distributions and is not supported by GSX Server.

If you have an X server based on XFree86 version 3.3.3.0, you cannot move the mouse while in full screen mode with the VidMode extension enabled. To resolve the problem, either disable video resolution switching in GSX Server or update your X server.

To disable video resolution switching in GSX Server, choose **Settings** > **Configuration Editor**, and deselect **Find best resolution** in the **Misc** panel.

Configuring Sound in GSX Server

GSX Server provides a Creative Labs Sound Blaster 16 compatible audio device and supports sound in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Server 2003 and Linux guest operating systems. The GSX Server sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**). Sound support is currently limited to PCM (pulse code modulation) output (that is, any application that produces sound without using MIDI).

Setting Up a Virtual Sound Card on a Windows Host

1. Be sure your physical sound card is installed and configured properly on the Windows host operating system. Refer to the documentation for your particular Windows operating system. You may need to install additional software on your system to support sound. VMware cannot provide support assistance in configuring sound on your host operating system. Please contact your host operating system support provider or sound card manufacturer for help.
2. Add a virtual sound adapter to the virtual machine. By default, the virtual sound adapter is not installed in the virtual machine.
3. In the Configuration Editor (**Settings** > **Configuration Editor**), click **Add**. The Add Hardware Wizard appears.
4. Select **Sound Adapter**, then click **Next**.

   If you have more than one physical sound adapter in your host computer, you can choose which one to connect to the virtual sound adapter. You can also choose whether the virtual sound adapter should be connected when the virtual machine starts.
5. Click **Finish**.
6. Click **OK** to close the Configuration Editor.
7. Configure the guest operating system to use the GSX Server virtual sound adapter. This adapter is compatible with a Creative Labs Sound Blaster 16.

Setting Up a Virtual Sound Card on a Linux Host

1. Be sure your physical sound card is installed and configured properly on the Linux host operating system. Refer to the documentation for your particular Linux operating system. You may need to install additional software on your system to support sound. VMware cannot provide support assistance in configuring sound on your host operating system. Please contact your host operating system support provider or sound card manufacturer for help.
2. Add a virtual sound adapter to the virtual machine. By default, the virtual sound adapter is not installed in the virtual machine.
3. In the Configuration Editor (**Settings** > **Configuration Editor**), click **Sound**.
4. Provide the device name in the **Device** field. Type in or browse to the device that represents your sound card (for example, `/dev/dsp`).
5. Click the **Install** button, then click **OK** to save the configuration and close the Configuration Editor.

Setting Up Sound in the Guest Operating System

Use your guest operating system's configuration tools to set up the virtual sound adapter.

Sound in a Windows XP or Windows Server 2003 Guest

1. Open the Windows XP or Windows Server 2003 Control Panel (choose **Start** > **Control Panel**), then click the **Printers and Other Hardware** link.
2. In the See Also pane, click **Add Hardware**, then click **Next**.
3. Select **Yes, I have already connected the hardware**, then click **Next**.
4. In the Installed Hardware list, select **Add a new hardware device**, then click **Next**.
5. Select **Install the hardware that I manually select from a list (Advanced)**, then click **Next**.
6. Select **Sound, video and game controllers**, then click **Next**.
7. Select **Creative Technology Ltd.** in the Manufacturer list and **Sound Blaster 16 or AWE32 or compatible (WDM)** in the list of devices, then click **Next**.
8. Click **Next**.
9. Click **Finish**.

Sound in a Windows 2000 Guest

1. Open the Windows 2000 Control Panel (choose **Start** > **Settings** > **Control Panel**), then double-click the **Add/Remove Hardware** icon.
2. In the Add/Remove Hardware Wizard dialog box, select **Add a New Device** and click **Next**.
3. In the Find New Hardware dialog box, select **No, I want to select the hardware from a list** and click **Next**.
4. In the Hardware Type dialog box, select **Sound, video and game controllers** from the list and click **Next**.
5. In the Select a Device Driver dialog box, select **Creative** from the manufacturers list and select **Sound Blaster 16 or AWE32 or compatible (WDM)** from the models list, then click **Next**.
6. In the Start Hardware Installation dialog box, click **Next** to install the Sound Blaster 16 drivers.
7. In the Completing the Add/Remove Hardware Wizard dialog box, click **Finish** and reboot the virtual machine. Sound should be working the next time the virtual machine boots Windows 2000.

Sound in a Windows NT Guest

If you have never installed a Sound Blaster 16 Card in this Windows NT system, you need a Windows NT 4.0 installation CD-ROM.

1. Open the Windows NT Control Panel (choose **Start** > **Settings** > **Control Panel**), then double-click the **Multimedia** icon.
2. Click the **Devices** tab.
3. Click the **Add** button.
4. Select the **Creative Labs Sound Blaster 1.X, Pro, 16**, then click **OK**.
5. Insert the Windows NT 4.0 CD-ROM in the CD-ROM drive when prompted.
6. Specify `D:\I386` (where `D:` is your CD-ROM drive), then click **OK**.
7. Configure the Sound Blaster base I/O Address.

I/O address
0x220

8. Click **OK**.

9. Complete the Sound Blaster 16 Configuration.

IRQ	8-bit DMA	16-bit DMA	MPU-401 I/O address
5	1	7	Disable (MPU-401 MIDI device is not supported)

   Click **OK**.

10. When prompted to restart, click **Restart Now**.

Sound in a Windows 95 or Windows 98 Guest

If you have never installed a Sound Blaster 16 Card in this Windows guest operating system, you need a Windows 95 or Windows 98 installation CD-ROM.

1. Open the Windows Control Panel (choose **Start** > **Settings** > **Control Panel**), double-click the **Add New Hardware** icon, then click **Next**.
2. Select **Yes** for **Do you want Windows to search for new hardware?**, then click **Next**.
3. Click **Next** again. Windows runs the autodetection and says it is ready to finish.
4. If prompted to do so, insert the Windows CD-ROM into the drive and click **OK**, then click **Finish**.

If you have problems with Windows autodetection, add the device manually.

1. Double-click the Add New Hardware icon in the Windows Control Panel (**Start** > **Settings** > **Control Panel**), then click **Next**.
2. Select **No** for **Do you want Windows to search for new hardware?**, then click **Next**.
3. Select **Sound, video and games controllers**, then click **Next**.
4. Select **Creative Labs Sound Blaster 16 or AWE-32**, then click **Next**.
5. Click **Finish**.

Sound in a Linux Guest

1. Refer to the documentation for your particular Linux distribution. You may need to install additional software packages on your system to support sound.
2. When configuring the sound, please use the following parameters:

I/O port	IRQ	8-bit DMA	16-bit DMA
0x220	5	1	7

Known Limitations of Sound Support in GSX Server

Sound support is provided for Sound Blaster compatible PCM (pulse code modulation) output. This gives you the ability to play `.wav`, `.au` and Real Audio formats, among others.

MIDI sound is not supported.

Game ports and devices such as joysticks attached to game ports are not supported.

Sound does not work well with certain games, especially fast, interactive games.

Sound is not supported in FreeBSD guest operating systems.

Improving Sound Performance

If you notice that sound skips in your guest operating system, you may try adding two variables to your virtual machine's configuration file (`.vmx` on Windows hosts, `.cfg` on Linux hosts). These variables are `sound.maxLength` and `sound.smallBlockSize`.

VMware cannot provide you with specific settings to use; how these settings affect your sound quality depends on many factors, including your environment and the way you are employing sound. But here are some general rules of thumb to use when setting these variables:

- Set these values to powers of 2, such as 64, 128 or 512.
- To overcome skipping, setting these values lower than 512 should help.
- The `sound.maxLength` setting should be greater than or equal to the `sound.smallBlockSize` setting.

14

Connecting Devices

Using Devices with a Virtual Machine

The following sections describe how to use various devices with a virtual machine:

- Using Parallel Ports on page 484
  - Unidirectional Ports on page 484
  - Bidirectional Ports on page 484
  - Default Configuration on page 485
  - Installation in Guest Operating Systems on page 485
  - Troubleshooting on page 488
  - Configuring a Bidirectional Parallel Port on a Linux Host on page 488
  - Devices You Can Use on a Bidirectional Parallel Port on page 491
- Using Serial Ports on page 492
  - Using a Serial Port on the Host Computer on page 492
  - Using a File on the Host Computer on page 494
  - Connecting an Application on the Host to a Virtual Machine on page 495
  - Connecting Two Virtual Machines on page 497
  - Special Configuration Options for Advanced Users on page 500
  - Usage Scenarios: Debugging Over a Virtual Serial Port on page 501
- Keyboard Mapping on a Linux Host on page 504
  - Quick Answers on page 504
  - The Longer Story on page 504
  - V-Scan Code Table on page 507
- Using USB Devices in a Virtual Machine on page 513
  - Notes on USB Support on page 513
  - Enabling and Disabling the USB Controller on page 513
  - Connecting USB Devices on page 513
  - Using USB with a Windows Host on page 514
  - Using USB with a Linux Host on page 514
  - Who Has Control Over a USB Device? on page 515
  - Disconnecting USB Devices from a Virtual Machine on page 516

- Human Interface Devices on page 516
- Connecting to a Generic SCSI Device on page 517
  - Device Support in Guest Operating Systems on page 517
  - Generic SCSI on a Windows Host Operating System on page 518
  - Generic SCSI on a Linux Host Operating System on page 519

Using Parallel Ports

GSX ServerGSX Server supports two types of virtual parallel port devices: unidirectional ports (SPP) and a partial emulation of bidirectional PS/2-style ports.

Bidirectional ports are supported on all Windows hosts. Unidirectional ports are not supported on Windows hosts.

Unidirectional ports are supported in all Linux kernel versions. Bidirectional ports are supported in Linux kernel versions 2.2.5 or later.

On Linux hosts, GSX Server requires that the parallel port "PC-style hardware" option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module (that is, it must be set to `"m"`). GSX Server cannot use bidirectional parallel port devices if `CONFIG_PARPORT_PC` is built directly (compiled) into the kernel. This limitation exists because `CONFIG_PARPORT_PC` does not correctly export its symbols.

The virtual parallel ports can be configured in two ways.

- You can connect a virtual parallel port to a physical parallel port on the host computer.
- You can connect a virtual parallel port to a file on the host computer.

Unidirectional Ports

Unidirectional ports are supported for backward compatibility. They are used typically to connect to printers or to send the printer output to a file. The speed is usually adequate for printing text, but expect long delays when printing images.

On a Linux host, the path names of the host devices for unidirectional ports are typically `/dev/lp0`, `/dev/lp1` and so on.

Unidirectional ports are not supported on Windows hosts.

Bidirectional Ports

Bidirectional ports are used by a variety of devices — printers, scanners, dongles and disk drives, for example.

Currently, GSX Server provides only partial emulation of PS/2 hardware. Specifically, interrupts requested by a device connected to the physical port are not passed to the virtual machine. Also, the guest operating system cannot use DMA (direct memory access) to move data to or from the port.

For this reason, not all devices that attach to the parallel port are guaranteed to work correctly. For a partial list of devices known to work, see Devices You Can Use on a

Bidirectional Parallel Port on page 491. If you try out a device that is not on the list, please let VMware know.

Bidirectional emulation is slower than native access but faster than unidirectional emulation, so bidirectional mode is recommended, when possible, even when the device connected to the port is unidirectional (a printer, for example).

Note: On a Linux host, you cannot start a virtual machine with a bidirectional parallel port connected, even if the device is set to start connected in the Configuration Editor. On a Windows host, the parallel port may disconnect when the guest operating system boots. When the guest operating system finishes booting, you can connect the port. In the console, choose **Devices** > **<parallel_port_name>** > **Connect**.

Default Configuration

When parallel ports are set up on a Windows host, they are bidirectional by default. Their default base addresses are, in order, 0x3bc, 0x378 and 0x278. None of the ports have an assigned IRQ or DMA channel. The ports are not present by default.

When parallel ports are set up on a Linux host, they are bidirectional by default on Linux hosts with kernel 2.2 or higher. Otherwise, they are unidirectional. Their default base addresses are in order, 0x3bc, 0x378 and 0x278. None of the ports have an assigned IRQ or DMA channel. The ports are not present by default.

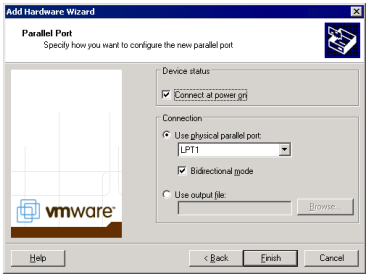
Installation in Guest Operating Systems

If the virtual machine is configured with a parallel port, most guest operating systems automatically detect it at installation time and install the required drivers. Some operating systems, including Linux, Windows NT and Windows 2000, automatically detect the port(s) at boot time. Others, like Windows 9x, do not.

To add a parallel port to the virtual machine's configuration, take these steps with the virtual machine powered off.

Windows Hosts

1. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
2. Click **Add** to start the New Hardware Wizard.
3. Select **Parallel Port**, then click **Next**.



4. Make the appropriate selection to use a physical parallel port or connect the virtual parallel port to a file. If you want the parallel port output to go to a file, enter the path and filename or browse to the location of the file.

   Note: If you are connecting with a Windows remote console to add a physical parallel port to a virtual machine on a Linux host, be sure to specify a Linux device name here, such as `/dev/paport0`.

5. Leave the **Connect at power on** option selected if you want the parallel port device to be available as soon as the virtual machine powers on.
6. Check **Bidirectional mode** if this parallel port is a bidirectional parallel port.
7. Click **Finish** to install the virtual parallel port, then click **OK** to save the configuration and close the Configuration Editor.
8. If this parallel port is bidirectional, enable it in the virtual machine's BIOS. When you boot the guest operating system, press F2 to enter the BIOS. Complete the following steps.

   A. Use the arrow keys to select **Advanced**, then scroll down to I/O Device Configuration and press Enter.

   B. Scroll down to Parallel Port and use the -/+ keys to select **Enabled**.

   C. Scroll down to Mode and use the -/+ keys to select **Bidirectional**.

   D. Press F10 to save the BIOS changes and exit the BIOS setup utility.

   E. Press **Reset** on the console toolbar to restart the guest operating system.

Linux Hosts

Before you can install a bidirectional parallel port in a virtual machine on a Linux host, you need to modify the host BIOS so it has the desired settings for the device you intend to install in the guest operating system. The settings you choose for the host (parallel port, bidirectional) must match the settings you will choose for the guest operating system and the virtual machine's BIOS in the following steps.

1. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
2. Click the **+** sign beside **Parallel Ports** to expand the list of devices.
3. Select a device that is shown as **Not Installed**.
4. From the **Type** drop-down list, select **Device** to connect to a physical parallel port on the host or **File** to send the output to a file.
5. In the **Path** field, enter the path to the device or file you want to use.

   The path names of the host devices for bidirectional parallel ports are usually `/dev/parport0`, `/dev/portport16`, `/dev/parport32`, and so on. The GSX Server installer creates these devices if they do not exist. They may also be created by hand using `mknod`. For example, to create the second parallel port (`parport16`) use this command:

   ```
   mknod /dev/parport16 c 99 16
   ```

   Note: If you are connecting with a Linux remote console to add a physical parallel port to a virtual machine on a Windows host, be sure to specify a Windows device name here, such as LPT1.
6. In the Parallel Port window, select the **Start Connected** option if you want the parallel port device to be available as soon as the virtual machine powers on.
7. Click **Install** to install the virtual parallel port, then click **OK** to save the configuration and close the Configuration Editor.
8. If this parallel port is bidirectional, enable it in the virtual machine's BIOS. When you boot the guest operating system, press F2 to enter the BIOS. Complete the following steps.
   A. Use the arrow keys to select **Advanced**, then scroll down to I/O Device Configuration and press Enter.
   B. Scroll down to Parallel Port and use the -/+ keys to select **Enabled**.
   C. Scroll down to Mode and use the -/+ keys to select **Bidirectional**.
   D. Press F10 to save the BIOS changes and exit the BIOS setup utility.
   E. Press **Reset** on the console toolbar to restart the guest operating system.

In a Windows 98 or Windows 95 guest, when you change a port from unidirectional to bidirectional or vice versa, you must use the Device Manager (**Start** > **Settings** > **Control Panel** > **System** > **Device Manager**) to remove the device driver for that port and add a new one. Adding a new driver is also required when a new port is added. In both cases use the guest operating system's Add New Hardware Wizard (**Start** > **Settings** > **Control Panel** > **Add New Hardware**) and let Windows detect the new device. Manually selecting the device from a list may result in an incorrect configuration.

Troubleshooting

If an error message appears at power on stating the parallel port on the host does not have an ECR (extended control register), it is possible the hardware supports it but it has been disabled in the BIOS. In this case, reboot your host computer, enter the BIOS configuration editor (typically by holding down the Delete key during early execution of the BIOS), find the parallel port field, and enable ECP mode (or other combination of modes that include ECP). Most modern computers should support ECP mode.

Configuring a Bidirectional Parallel Port on a Linux Host

For the bidirectional parallel port to work properly in a guest, it must first be configured properly on the host. Most issues involving parallel port functionality are a result of the host configuration. Check these areas of concern: the version of your Linux kernel, your device access permissions and required modules.

Bidirectional Parallel Ports and Linux 2.4.x Kernels

Be sure that PC Style Hardware (`CONFIG_PARPORT_PC`) is loaded as a module as mentioned at the beginning of this section on using parallel ports. If you are using a 2.4.x kernel, the modules that provide bidirectional parallel port functionality are `parport`, `parport_pc` and `ppdev`.

To see if these modules are installed and running on your system, run the `lsmod` command as the root user. These three modules should be included in the listing of running modules. You can also look at the `/proc/modules` file for the same list.

To load the proper modules, run this command:

```
insmod -k <modulename>
```

If none of the listed parallel port modules is running, use this command:

```
insmod -k parport_pc
```

This inserts the three modules needed for a bidirectional parallel port.

If you continue to see problems, it is possible that the `lp` module is running. If it is, the virtual machine cannot use the parallel port correctly. To remove the `lp` module, run this command as the root user:

```
rmmod lp
```

The `lp` module is necessary only for unidirectional parallel ports.

You should also ensure that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a `#` at the beginning of the line. The name of the configuration file depends on the Linux distribution you are using. When you reboot the host after removing this line, the configuration file no longer starts the `lp` module.

To ensure that the proper modules for the bidirectional parallel port are loaded at boot time, add this line to `/etc/modules.conf` or `/etc/conf.modules`:

```
alias parport_lowlevel parport_pc
```

Linux kernels in the 2.4.x series also use a special arbitrator that allows access to the parallel port hardware. If the parallel port is in use by the host, the guest cannot use it. If a virtual machine is using the parallel port, the host and any users accessing the host are not given access to the device. GSX Server puts a lock on the device, and this lock restricts access so only the virtual machine can use the port.

You can use the **Devices** menu to disconnect the parallel port from the virtual machine and reconnect it.

Bidirectional Parallel Ports and Linux 2.2.x Kernels

The 2.2.x kernels that support bidirectional parallel ports use the `parport`, `parport_pc` and `vmppuser` modules. Also, be sure that PC Style Hardware (`CONFIG_PARPORT_PC`) is loaded as a module, as mentioned at the beginning of this section on using parallel ports. The `vmppuser` module is supplied by GSX Server to give virtual machines user-level access to the parallel port.

To see if these modules are installed and running on your system, run the `lsmod` command as the root user. These three modules should be included in the listing of running modules. You can also look at the `/proc/modules` file for the same list.

To load the proper modules, run this command:

```
insmod -k <modulename>
```

If none of the listed parallel port modules is running, use this command:

```
insmod -k parport_pc
```

This inserts the three modules needed for a bidirectional parallel port.

If you continue to see problems, it is possible that the `lp` module is running. If it is, the virtual machine cannot use the parallel port correctly. To remove the `lp` module, run this command as the root user:

```
rmmod lp
```

The `lp` module is necessary only for unidirectional parallel ports.

You should also ensure that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a # at the beginning of the line. The name of the configuration file depends on the Linux distribution you are using. When you reboot the host after removing this line, the configuration file no longer starts the `lp` module.

To ensure that the proper modules for the bidirectional parallel port are loaded at boot time, add this line to `/etc/modules.conf` or `/etc/conf.modules`:

```
alias parport_lowlevel parport_pc
```

Device Permissions

Some Linux distributions by default do not grant the virtual machine access to the `lp` and `parport` devices. In most of these cases, the owner of the device is `root` and the associated group is `lp`. To allow the GSX Server user to access the device, add the user to the associated group. To view the owner and group of the device, run this command:

```
ls –la /dev/parport0
```

The third and fourth columns of the output show the owner and group, respectively.

To add the user to the device group, edit the `/etc/group` file. On the line starting with `lp`, which defines the `lp` group, add the GSX Server user's user name. You must make this change as the root user. The following line provides an example for a user whose user name is `userj`.

```
lp::7:daemon,lp,userj
```

The next time the user logs on to the host, the changes take effect.

Devices You Can Use on a Bidirectional Parallel Port

Devices Known to Work

Adobe dongle	Windows 95 guest
RIO MP3 player	Windows 95 guest
UMAX Astra 1220 P scanner	Windows 95 guest
Hewlett-Packard LaserJet 5MP printer	Windows 95, Windows 98, Windows NT and Windows 2000 guests
Canon Bubble Jet BJ-200e printer	Windows 95, Windows 98, Windows NT and Windows 2000 guests
Iomega ZIP drive	Linux, Windows NT and Windows 2000 guest only (see Special Notes for the Iomega Zip Drive, below)

Devices That Probably Work

Dongles	Most dongles are likely to work.
Printers	Most printers are likely to work.
Hewlett-Packard Deskjet 710C	Reported by customer.
Hewlett-Packard Deskjet 722C	Reported by customer.
Epson 750 printer in bidirectional mode	Reported by customer.
CARDport Swift Smart Media Digital Image Reader/Writer from Chase Advanced Technologies	Reported by customer.
Logitech Scanman Color 2000 (parallel port hand scanner)	Reported by customer.
Plustek Optic Pro 9636T Flatbed Scanner	Reported by customer.
Creative Labs WebCam II (parport version)	Reported by customer.

Special Notes for the Iomega Zip Drive

On Windows 98 or Windows 95, use of older drivers for the Iomega Zip drive may cause the guest operating system to lock up intermittently at boot time or during installation of the guest operating system. The newest Iomega drivers work reliably in our tests. They are available at *www.iomega.com/software/index.html*.

Using Serial Ports

GSX ServerA GSX Server virtual machine can use up to four virtual serial ports. The virtual serial ports can be configured in several ways.

- You can connect a virtual serial port to a physical serial port on the host computer.
- You can connect a virtual serial port to a file on the host computer.
- You can make a direct connection between two virtual machines or between a virtual machine and an application running on the host computer.

You can also select whether to connect the virtual serial port when you power on the virtual machine.

Note: As of GSX Server 2, the use of TTY type of virtual serial ports in a virtual machine has been deprecated.

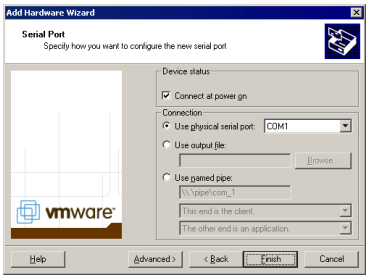
Using a Serial Port on the Host Computer

You can set up the virtual serial port in a virtual machine to use a physical serial port on the host computer. This is useful, for example, if you want to use an external modem or a hand-held device in your virtual machine.

To install a virtual serial port that connects to a physical serial port on the host computer, take the following steps:

Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use Physical Serial Port**, then choose the port on the host computer that you want to use for this serial connection.

Note: If you are connecting with a Windows remote console to add a physical serial port to a virtual machine on a Linux host, be sure to specify a Linux device name here, such as `/dev/ttyS0`.

5. Click **Finish**, then click **OK** to close the Configuration Editor.
6. Power on the virtual machine.

Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose **Device** from the **Type** pull-down menu.
4. In the **Path** field, enter the path to the device you want to connect to the virtual serial port, for example, `/dev/ttyS0` to use the first physical serial port on the host computer.

   Note: If you are connecting with a Linux remote console to add a physical serial port to a virtual machine on a Windows host, be sure to specify a Windows device name here, such as COM1.
5. Click **Install**.
6. Click **OK** to save your configuration and close the Configuration Editor.
7. Power on the virtual machine.

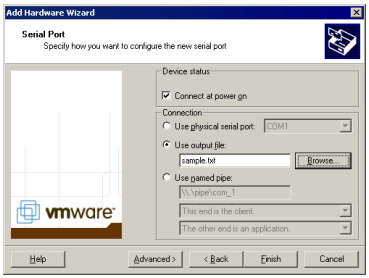
Using a File on the Host Computer

You can set up the virtual serial port in a virtual machine to send its output to a file on the host computer. This is useful, for example, if you want to capture the data a program running in the virtual machine sends to the virtual serial port or if you need a quick way to transfer a file from the guest to the host.

To install a virtual serial port that connects to a file on the host computer, take the following steps:

Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use output file** and browse to the file on the host computer that you want to use to store the output of the virtual serial port.
5. Click **Finish**, then click **OK** to close the Configuration Editor.
6. Power on the virtual machine.

Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose **File** from the **Type** pull-down menu.
4. In the **Path** field, enter the path to the file on the host computer that you want to use to store the output of the virtual serial port.
5. Click **Install**.
6. Click **OK** to save your configuration and close the Configuration Editor.
7. Power on the virtual machine.

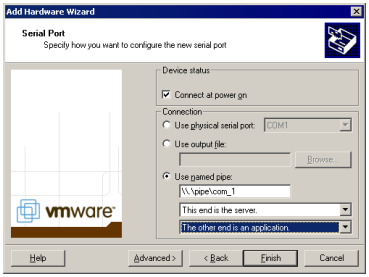
Connecting an Application on the Host to a Virtual Machine

You can set up the virtual serial port in a virtual machine to connect to an application on the host computer. This is useful, for example, if you want to use an application on the host to capture debugging information sent from the virtual machine's serial port.

To install a direct serial connection between an application on the host and a virtual machine, take the following steps:

Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use named pipe**.
5. Use the default pipe name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`.

   Note: If you are using a Windows remote console to connect to a virtual machine on a Linux host, be sure to specify a Linux pipe name here, such as `/tmp/<pipe>`.
6. Select **This end is the server** or **This end is the client**. In general, select **This end is the server** if you plan to start this end of the connection first.
7. Select **The other end is an application**.
8. Click **Finish**, then click **OK** to close the Configuration Editor.
9. On your host computer, configure the application that communicates with the virtual machine to use the same pipe name.
10. Power on the virtual machine.

Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Pipe** from the pull-down menu.
4. In the **Path** field, enter `/tmp/<pipe>` as the name of the pipe.

   Note: If you are using a Linux remote console to connect to a virtual machine on a Windows host, be sure to specify a Windows pipe name here, such as `\\.\pipe\<namedpipe>`.
5. Select **Server** or **Client**. In general, select **Server** if you plan to start this end of the connection first.
6. Click **Install**.
7. Click **OK** to save your configuration and close the Configuration Editor.
8. On your host computer, configure the application that communicates with the virtual machine to use the same pipe name.
9. Power on the virtual machine.

Connecting Two Virtual Machines

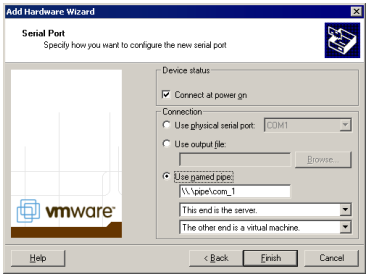
You can set up the virtual serial ports in two virtual machines to connect to each other. This is useful, for example, if you want to use an application in one virtual machine to capture debugging information sent from the other virtual machine's serial port.

To install a direct serial connection between two virtual machines (a server and a client), take the following steps:

Windows Host

In the server virtual machine

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.

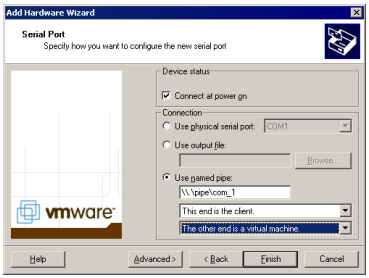


4. Select **Use named pipe**.
5. Use the default pipe name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`.

   Note: If you are using a Windows remote console to connect to a virtual machine on a Linux host, be sure to specify a Linux pipe name here, such as `/tmp/<pipe>`.
6. Select **This end is the server**.
7. Select **The other end is a virtual machine**.
8. Click **Finish**, then click **OK** to close the Configuration Editor.

In the client virtual machine

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use named pipe**.
5. Use the default name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`. The pipe name must be the same on server and client.

   Note: If you are using a Windows remote console to connect to a virtual machine on a Linux host, be sure to specify a Linux pipe name here, such as `/tmp/<pipe>`.
6. Select **This end is the client**.
7. Select **The other end is a virtual machine**.
8. Click **Finish**, then click **OK** to close the Configuration Editor.

Linux Host

In the server virtual machine

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Pipe** from the pull-down menu.
4. In the **Path** field, enter `/tmp/<pipe>` as the name of the pipe.

   Note: If you are using a Linux remote console to connect to a virtual machine on a Windows host, be sure to specify a Windows pipe name here, such as `\\.\pipe\<namedpipe>`.
5. Select **Server**.
6. Click **Install**.
7. Click **OK** to save your configuration and close the Configuration Editor.

In the client virtual machine

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Pipe** from the pull-down menu.
4. In the **Path** field, enter `/tmp/<pipe>` as the name of the pipe. The pipe name must be the same on server and client.

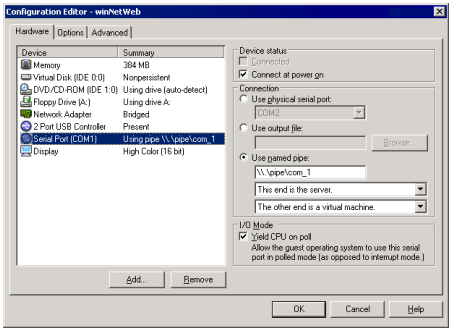
   Note: If you are using a Linux remote console to connect to a virtual machine on a Windows host, be sure to specify a Windows pipe name here, such as `\\.\pipe\<namedpipe>`.
5. Select **Client**.
6. Click **Install**.
7. Click **OK** to save your configuration and close the Configuration Editor.

Special Configuration Options for Advanced Users

Two special configuration options are available for serial connections between a virtual machine and the host or between two virtual machines. These options are of interest primarily to developers who are using debugging tools that communicate over a serial connection.

Improving CPU Performance when Debugging

The first option must be set in the Configuration Editor. It is useful when the serial port is being used by the guest operating system in polled mode as opposed to interrupt mode. Polled mode causes the virtual machine to consume a disproportionate share of CPU time. This makes the host and other guests run sluggishly.



To restore performance for applications on the host, in the Configuration Editor, select the virtual serial port, and check the **Yield CPU on poll** check box. This configuration option forces the affected virtual machine to yield processor time if the only thing it is trying to do is poll the virtual serial port.

Changing the Input Speed of the Serial Connection

The second option — `serial<n>.pipe.charTimePercent = <x>` — should be added as a new line to your virtual machine's configuration file. It is useful to squeeze every possible bit of speed from your serial connection over a pipe to the virtual machine. GSX Server does not impose a limit on the output speed, which is how fast the virtual machine sends data through the virtual serial port. The output speed depends on how fast the application at the other end of the pipe reads data inbound to it.

`<n>` is the number of the serial port, starting from `0`. So the first serial port is `serial0`. `<x>` is any positive integer. It specifies the time taken to transmit a character, expressed as a percentage of the default speed set for the serial port in the

guest operating system. For example, a setting of 200 forces the port to take twice as long per character, or send data at half the default speed. A setting of 50 forces the port to take only half as long per character, or send data at twice the default speed.

You should first use the guest operating system to configure the serial port for the highest setting supported by the application you are running in the virtual machine.

Once the serial port speed is set appropriately in the guest operating system, experiment with this setting. Start with a value of 100 and gradually decrease it until you find the highest speed at which your connection works reliably.

Usage Scenarios: Debugging Over a Virtual Serial Port

You can use Debugging Tools for Windows (WinDbg) or Kernel Debugger (KD) to debug kernel code in a virtual machine over a virtual serial port. You can download Debugging Tools for Windows from the Windows DDK Web site at *www.microsoft.com/whdc/ddk/*.

The following two examples illustrate how to use a virtual serial port to debug kernel code in a virtual machine:

- Where the debugging application is on the GSX Server host (Windows hosts only)
- Where the debugging application is in another virtual machine on the same GSX Server host (which is useful on a Linux host, but can also be done on a Windows host)

Using either of these methods lets you debug kernel code on one system, without the need for two physical computers, a modem or serial cable.

Debugging an Application in a Virtual Machine from the Windows Host

In this situation, you have kernel code to debug in a virtual machine (called the target virtual machine) and are running WinDbg or KD on your Windows host.

To prepare the target virtual machine, follow the steps for a Windows host in Connecting an Application on the Host to a Virtual Machine on page 495. Make sure you configure the virtual machine's virtual serial port as follows:

- Select **This end is the server**
- Under **I/O Mode**, select the **Yield CPU on poll** check box, as the kernel in the target virtual machine uses the virtual serial port in polled mode, not interrupt mode

To prepare the host, make sure you have downloaded the correct version of Debugging Tools for Windows. You need version 4.0.18.0, dated December 21, 2001, or later, which support debugging over a pipe.

Note: Pipe support is not documented in the `WinDbg` and `KD` in-product help or on Microsoft's Web site.

When you are ready to begin, complete the following steps:

1. Power on the virtual machine.
2. Check to make sure the serial port is connected. On the **Devices** menu, **serial<n>** should say **Connecting…**, as it is waiting to connect to the host on the other end of the pipe.

   Note: If **serial<n>** says **(Not connected)**, then the serial port may not be connected. Choose the virtual serial port, then **Connect**.
3. On the host, open a Command Prompt window and do one of the following:
   - If you are using `WinDbg`, type the following:

     ```
     windbg -k com:port=\\.\pipe\<namedpipe>,pipe
     ```
   - If you are using `KD`, type the following:

     ```
     kd -k com:port=\\.\pipe\<namedpipe>,pipe
     ```

   Then press `Enter` to start debugging.

Debugging an Application in a Virtual Machine from another Virtual Machine

In this situation, you have kernel code to debug in a virtual machine (called the target virtual machine) and are running Debugging Tools for Windows (`WinDbg`) or Kernel Debugger (`KD`) in another virtual machine (called the debugger virtual machine) on the same host.

This is useful if you are running GSX Server on a Linux host. The debugger virtual machine must be running Debugging Tools for Windows (`WinDbg`) or Kernel Debugger (`KD`) in a Windows guest operating system.

To prepare the target virtual machine, follow the steps for the **server** virtual machine for the appropriate host in Connecting Two Virtual Machines on page 497. Make sure when you configure the target virtual machine's virtual serial port that you select the **Yield CPU on poll** check box, as the kernel in the target virtual machine uses the virtual serial port in polled mode, not interrupt mode.

To prepare the debugger virtual machine, make sure you have downloaded Debugging Tools for Windows. Then follow the steps for the **client** virtual machine in Connecting Two Virtual Machines on page 497.

When you are ready to begin, complete the following steps:

1. Power on both virtual machines.
2. Check to make sure the serial port is connected in each virtual machine. On the **Devices** menu, **serial<n>** should say **\\.\pipe\<namedpipe>** (Windows hosts) or **/tmp/<pipe>** (Linux hosts).

   Note: If the **serial<n>** says **(Not connected)**, then the serial port may not be connected. Choose the virtual serial port, then **Connect**.
3. In the debugger virtual machine, start debugging with `WinDbg` or `KD` normally.

Keyboard Mapping on a Linux Host

This section addresses the following issues and provides additional details on keyboard mapping in Linux:

- My (language-specific) keyboard is not supported by GSX Server.
- Some of the keys on my keyboard don't work right in the virtual machine.
- My keyboard works fine when I run a virtual machine locally, but not when I run the same virtual machine with a remote X server.

Quick Answers

If your keyboard works correctly with a local X server, and you just want the same behavior with a remote X server (which is also an XFree86 server running on a PC), just add the line

```
xkeymap.usekeycodeMapIfXFree86 = true
```

to the virtual machine configuration file or to `~/.vmware/config`. Make this change on the host machine, where you run the virtual machine, not on the machine with the remote X server.

If you are using an XFree86-based server that GSX Server does not recognize as an XFree86 server, use this instead:

```
xkeymap.usekey codeMap = true
```

If you are using an XFree86 server running locally, and the keyboard does not work correctly, please report the problem by submitting a support request at *www.vmware.com/requestsupport*.

The Longer Story

Unfortunately, keyboard support for the PC (virtual or otherwise) is a complex affair. To do it justice, we have to start with some background information — greatly simplified.

Pressing a key on the PC keyboard generates a scan code based roughly on the position of the key. For example, the Z key on a German keyboard generates the same code as the Y key on an English keyboard, because they are in the same position on the keyboard. Most keys have one-byte scan codes, some keys have two-byte scan codes with prefix 0xe0.

Internally, GSX Server uses a simplified version of the PC scan code that is a single 9-bit numeric value, called a v-scan code. A v-scan code is written as a three-digit hexadecimal number. The first digit is 0 or 1. For example, the left-hand Ctrl key has a

one-byte scan code (0x1d); its v-scan code is 0x01d. The right-hand Ctrl key scan code is two bytes (0xe0, 0x1d); its v-scan code is 0x11d.

An X server uses a two-level encoding of keys. An X key code is a one-byte value. The assignment of key codes to keys depends on the X server implementation and the physical keyboard. As a result, an X application normally cannot use key codes directly. Instead, the key codes are mapped into keysyms that have names like space, escape, x and 2. The mapping can be controlled by an X application via the function `XChangeKeyboardMapping()` or by the program `xmodmap`. To explore keyboard mappings, you can use `xev`, which shows the key codes and keysyms for keys typed into its window.

To recap, a key code corresponds roughly to a physical key, while a keysym corresponds to the symbol on the key top. For example, with an XFree86 server running on a PC, the Z key on the German keyboard has the same key code as the Y key on an English keyboard. The German Z keysym, however, is the same as the English Z keysym, and different from the English Y keysym.

For an XFree86 server on a PC, there is a one-to-one mapping from X key codes to PC scan codes (or v-scan codes, which is what GSX Server really uses). GSX Server takes advantage of this fact. When it is using an XFree86 server on the local host, it uses the built-in mapping from X key codes to v-scan codes. This mapping is keyboard independent and should be correct for most, if not all, languages. In other cases (not an XFree86 server or not a local server), GSX Server must map keysyms to v-scan codes, using a set of keyboard-specific tables.

Key code mapping is simple, automatic and foolproof. (Keysym mapping is more complex and described later.) However, because the program cannot tell whether a remote server is running on a PC or on some other kind of computer, it errs on the safe side and uses key code mapping only with local X servers. This is often too conservative and has undesirable effects. Luckily, this and other behavior related to key code-mapping can be controlled by using a text editor to add configuration settings to the virtual machine's configuration file.

- `xkeymap.usekeycodeMapIfXFree86 = true`
  Use key code mapping if using an XFree86 server, even if it is remote.
- `xkeymap.usekeycodeMap = true`
  Always use key code mapping regardless of server type.
- `xkeymap.nokeycodeMap = true`
  Never use key code mapping.

- `xkeymap.keycode.<code> = <v-scan code>`
  If using key code mapping, map key code `<code>` to `<v-scan code>`. In this example, `<code>` must be a decimal number and `<v-scan code>` should be a C-syntax hexadecimal number (for example, `0x001`).

The easiest way to find the X key code for a key is to run `xev` or `xmodmap -pk`. Most of the v-scan codes are covered in V-Scan Code Table on page 507. The keysym mapping tables described below are also helpful.

Use this feature to make small modifications to the mapping. For example, to swap left control and caps lock, use the following lines:

```
xkeymap.key code.64 = 0x01d # X Caps_Lock -> VM left ctrl
xkeymap.key code.37 = 0x03a # X Control_L -> VM caps lock
```

These configuration lines can be added to the individual virtual machine configuration, to your personal GSX Server configuration (`~/.vmware/config`), or even to the host-wide (`/etc/vmware/config`) or installation-wide (usually `/usr/local/lib/vmware/config`) configuration.

When key code mapping cannot be used (or is disabled), GSX Server maps keysyms to v-scan codes. This is done using one of the tables in the `xkeymap` directory in the GSX Server installation (usually `/usr/local/lib/vmware`).

Which table you should use depends on the keyboard layout. The normal distribution includes tables for PC keyboards for the United States and a number of European countries and languages. And for most of these, there are both the 101-key (or 102-key) and the 104-key (or 105-key) variants.

GSX Server automatically determines which table to use by examining the current X keymap. However, its heuristics may sometimes fail. In addition, each mapping is fixed and may not be completely right for any given keyboard and X key code-to-keysym mapping. For example, a user may have swapped control and caps lock using `xmodmap`. This means the keys are swapped in the virtual machine when using a remote server (keysym mapping) but unswapped when using a local server (key code mapping).

Therefore, keysym mapping is necessarily imperfect. To make up for this defect, most of the behavior can be changed with configuration settings:

- `xkeymap.language = <keyboard-type>`
  Use this if GSX Server has a table in `xkeymap` for your keyboard but can't detect it. `<keyboard-type>` must be one of the tables in the `xkeymap` directory. (See above for location.) However, the failure to detect the keyboard probably means the table isn't completely correct for you.

- `xkeymap.keysym.<sym> = <v-scan code>`
  If you use keysym mapping, map keysym `<sym>` to `<v-scan code>`. When you do, `<sym>` must be an X keysym name and `<v-scan code>` should be a C-syntax hexadecimal number (for example, `0x001`).

  The easiest way to find the keysym name for a key is to run `xev` or `xmodmap -pk`.

  The X header file `/usr/X11R6/include/X11/keysymdef.h` has a complete list of keysyms. (The name of a keysym is the same as its C constant without the XK_ prefix.) Most v-scan codes are in V-Scan Code Table on page 507.

  The `xkeymap` tables themselves are also helpful. Use them to fix small errors in an existing mapping.
- `xkeymap.fileName = <file-path>`
  Use the keysym mapping table in `<file-path>`. A table is a sequence of configuration lines of the form
  `<sym> = <v-scan code>`
  where `<sym>` is an X keysym name, and `<v-scan code>` is a C-syntax hexadecimal number (for example, `0x001`). (See the explanation of `xkeymap.keysym` above for tips on finding the keysyms and v-scan codes for your keyboard.)

  Compiling a complete keysym mapping is hard. It is best to start with an existing table and make small changes.

V-Scan Code Table

These are the v-scan codes for the 104-key U.S. keyboard:

Symbol	Shifted symbol	Location	V-scan code
Esc			0x001
1	!		0x002
2	@		0x003
3	#		0x004
4	$		0x005
5	%		0x006

Symbol	Shifted symbol	Location	V-scan code
6	^		0x007
7	&		0x008
8	*		0x009
9	(		0x00a
0	)		0x00b
-	_		0x00c
=	+		0x00d
Backspace			0x00e
Tab			0x00f
Q			0x010
W			0x011
E			0x012
R			0x013
T			0x014
Y			0x015
U			0x016
I			0x017
O			0x018
P			0x019
[	{		0x01a
]	}		0x01b
Enter			0x01c
Ctrl		left	0x01d

Symbol	Shifted symbol	Location	V-scan code
A			0x01e
S			0x01f
D			0x020
F			0x021
G			0x022
H			0x023
J			0x024
K			0x025
L			0x026
;			0x027
'			0x028
`			0x029
Shift		left	0x02a
\	|		0x02b
Z			0x02c
X			0x02d
C			0x02e
V			0x02f
B			0x030
N			0x031
M			0x032
,	<		0x033
.	>		0x034

Symbol	Shifted symbol	Location	V-scan code
/	?		0x035
Shift		right	0x036
*		numeric pad	0x037
Alt		left	0x038
Spacebar			0x039
Caps Lock			0x03a
F1			0x03b
F2			0x03c
F3			0x03d
F4			0x03e
F5			0x03f
F6			0x040
F7			0x041
F8			0x042
F9			0x043
F10			0x044
Num Lock		numeric pad	0x045
Scroll Lock			0x046
Home	7	numeric pad	0x047
Up arrow	8	numeric pad	0x048
PgUp	9	numeric pad	0x049
-		numeric pad	0x04a
Left arrow	4	numeric pad	0x04b

Symbol	Shifted symbol	Location	V-scan code
5		numeric pad	0x04c
Right arrow	6	numeric pad	0x04d
+		numeric pad	0x04e
End	1	numeric pad	0x04f
Down arrow	2	numeric pad	0x050
PgDn	3	numeric pad	0x051
Ins	0	numeric pad	0x052
Del		numeric pad	0x053
F11			0x057
F12			0x058
Break	Pause		0x100
Enter		numeric pad	0x11c
Ctrl		right	0x11d
/		numeric pad	0x135
SysRq	Print Scrn		0x137
Alt		right	0x138
Home		function pad	0x147
Up arrow		function pad	0x148
Page Up		function pad	0x149
Left arrow		function pad	0x14b
Right arrow		function pad	0x14d
End		function pad	0x14f
Down arrow		function pad	0x150

Symbol	Shifted symbol	Location	V-scan code
Page Down		function pad	0x151
Insert		function pad	0x152
Delete		function pad	0x153
Windows		left	0x15b
Windows		right	0x15c
Menu			0x15d

The 84-key keyboard has a Sys Req on the numeric pad:

Symbol	Shifted symbol	Location	V-scan code
Sys Req		numeric pad	0x054

Keyboards outside the U.S. usually have an extra key (often < > or < > |) next to the left shift key:

Symbol	Shifted symbol	Location	V-scan code
<	>		0x056

Using USB Devices in a Virtual Machine

You can use up to two USB devices in your virtual machine if both your host operating system and your guest operating system support USB. Note, for example, that Windows NT and Linux kernels older than 2.2.17 do not support USB.

Although your host operating system must support USB, you do not need to install drivers for your USB devices in the host operating system if you want to use those devices only in the virtual machine.

To take advantage of the USB support, you must create your virtual machine using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) in GSX Server.

Notes on USB Support

We have tested a variety of USB devices with this release. In general, if the guest operating system has appropriate drivers, you should be able to use PDAs, printers, storage (disk) devices, scanners, MP3 players, PC radios, digital cameras and memory card readers.

Modems and certain streaming data devices, such as Web cams, may not work properly.

Enabling and Disabling the USB Controller

A virtual machine's USB ports are enabled by default. If you are not using USB devices in a virtual machine, you can disable its USB controller in the Configuration Editor.

Connecting USB Devices

When a virtual machine is running, its window is the active window and a USB device is plugged into the host computer, the device automatically connects to the guest instead of the host. This autoconnect feature can be disabled in the USB Controller panel of the Configuration Editor (**Settings** > **Configuration Editor**). If all of the virtual machine's USB ports are already occupied when it is trying to connect automatically to a new device, a dialog box gives you a choice: you can either disconnect one of the existing USB devices to free its port or ignore the new device, allowing the device to connect to the host.

Use the **Devices** menu to connect specific USB devices to your virtual machine. You can connect up to two USB devices at a time. If the physical USB devices are connected to the host computer through a hub, the virtual machine sees only the USB devices, not the hub.

There is a menu item for each of the USB ports. Move the mouse over one of these items to see a cascading menu of devices that are plugged into your host computer and available for use. To connect a device to the virtual machine, click its name.

If a device is already connected to that port, clicking the name of a new device releases the first device, then connects the new one.

To release a connected device, click **None** on the cascading menu for the port to which it is connected.

If you physically plug a new device into the host computer and the autoconnect feature does not connect it to a virtual machine, the device is initially connected to the host. Its name is also added to the **Devices** menu so you can connect it to the virtual machine manually.

Using USB with a Windows Host

On Windows 2000 and Windows Server 2003 hosts, when a particular USB device is connected to a virtual machine for the first time, the host detects it as a new device named VMware USB Device and installs the appropriate VMware driver. On a Windows Server 2003 host, user confirmation is required in the Found New Hardware Wizard. Select the default action — **Install the software automatically**. Once this step completes, the guest operating system detects the USB device and searches for a suitable driver.

When you are synchronizing a PDA such as a Palm handheld or Handspring Visor to a virtual machine for the first time, the total time required to load the VMware USB device driver in the host and the PDA driver in the guest may exceed the device's connection timeout value. This causes the device to disconnect itself from the computer before the guest can synchronize with it. If this occurs, let the guest finish installing the PDA driver, dismiss any connection error warnings, then try synchronizing the PDA again. The second attempt should succeed.

Using USB with a Linux Host

On Linux hosts, GSX Server uses the USB device file system to connect to USB devices. In most Linux systems that support USB, the USB device file system is at `/proc/bus/usb`. If your host operating system uses a different path to the USB device file system, you can change it in the Configuration Editor (**Settings** > **Configuration Editor** > **USB**). Enter the correct path in the **Path to usbdevfs** field.

Who Has Control Over a USB Device?

Only one computer — host or virtual machine — can have control of a USB device at any one time.

Device Control on a Windows Host

When you connect a device to a virtual machine, it is "unplugged" from the host or from the virtual machine that previously had control of the device. When you disconnect a device from a virtual machine, it is "plugged in" to the host.

Caution: On Windows 2000 and Windows Server 2003 hosts, you need to take a special step to disconnect USB network and storage devices from the host. There is a system tray icon called Eject Hardware on Windows 2000 and Safely Remove Hardware on Windows Server 2003. Use this icon to disconnect the device from the host before connecting it to a virtual machine.

Device Control on a Linux Host

On Linux hosts, guest operating systems can use devices that are not already in use by the host — that is, claimed by a host operating system driver.

If your device is in use by the host and you try to connect it to the guest using the **Devices** menu, a dialog box appears, informing you that there is a problem connecting to the device.

To disconnect the device from the host, you must unload the device driver. You can unload the driver manually as root (`su -`) using the `rmmod` command. Or, if the driver was automatically loaded by `hotplug`, you can disable it in the `hotplug` configuration files in the `/etc/hotplug` directory. See your Linux distribution's documentation for details on editing these configuration files.

A related issue sometimes affects devices that rely on automatic connection (as PDAs often do).

If you have successfully used autoconnection to connect the device to your virtual machine, then experience problems with the connection to the device, take the following steps:

1. Disconnect and reconnect the device. You can either unplug it physically, then plug it back in or use the **Devices** menu to disconnect it and reconnect it.
2. If you see a dialog box warning that the device is in use, disable it in the `hotplug` configuration files in the `/etc/hotplug` directory.

Disconnecting USB Devices from a Virtual Machine

Before unplugging a USB device or using the **Devices** menu to disconnect it from a virtual machine, be sure it is in a safe state.

You should follow the procedures the device manufacturer specifies for unplugging the device from a physical computer. This is true whether you are physically unplugging it, moving it from host to virtual machine, moving it between virtual machines or moving it from virtual machine to host.

This is particularly important with data storage devices (a Zip drive, for example). You may lose data if you move a data storage device too soon after saving a file and the operating system has not actually written the data to the disk.

Human Interface Devices

USB human interface devices, such as the keyboard and mouse, are not handled though the virtual machine's USB controller. Instead, they appear in the virtual machine as a standard PS/2 keyboard and mouse, even though they are plugged into USB ports on the host.

Connecting to a Generic SCSI Device

Generic SCSI lets a virtual machine run any SCSI device that is supported by the guest operating system in the virtual machine. Generic SCSI gives the virtual machine direct access to SCSI devices connected to the host, such as scanners and tape drives.

Device Support in Guest Operating Systems

In theory, generic SCSI is completely device independent, but VMware has discovered it is sensitive to the guest operating system, device class and specific SCSI hardware. We encourage you to try any SCSI hardware you want to use and report problems to VMware technical support.

Preparing a Windows XP or Windows Server 2003 Guest Operating System to Use SCSI Devices

To use SCSI devices in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions there to install the driver.

Preparing a Windows NT 4.0 Guest Operating System to Use SCSI Devices

Generic SCSI devices use the virtual Mylex (BusLogic) BT-958 compatible host bus adapter provided by the virtual machine. Some guest operating systems guide you through installing the drivers after you install the first SCSI device in the virtual machine. On Windows NT 4.0, however, you may need to install the driver manually, if it is not already installed for a virtual SCSI disk. You should do so before you add a generic SCSI device.

To install the BusLogic driver in a Windows NT 4.0 guest, have your Windows NT installation CD available and follow these steps.

1. Open the SCSI Adapters control panel.

   Start > **Settings** > **Control Panel** > **SCSI Adapters**
2. Click the **Drivers** tab.
3. Click **Add**.
4. In the list of vendors on the left, select **BusLogic**.
5. In the list of drivers on the right, select **BusLogic MultiMaster PCI SCSI Host Adapters**.
6. Click **OK**.
7. Insert the Windows NT CD when you are prompted. Click **OK**.
8. Reboot the guest operating system when you are prompted.

Preparing a Windows Me, Windows 98 or Windows 95 Guest Operating System to Use SCSI Devices

If you are using generic SCSI devices in a Windows 95, Windows 98 or Windows Me guest operating system and are experiencing problems with the devices, download the Mylex (BusLogic) BT/KT-958 compatible host bus adapter for Windows 95 from *www.lsilogic.com*. This driver overrides what Windows chooses as the best driver, but it corrects known problems.

Generic SCSI on a Windows Host Operating System

Using the SCSI Generic driver in Windows, GSX Server allows your guest operating system to operate generic SCSI devices — including scanners, tape drives and other data storage devices — in a virtual machine.

Adding a Generic SCSI Device to a Virtual Machine

You can add generic SCSI devices to your virtual machine in the Configuration Editor. When you set up a generic SCSI device, make sure the device is connected to the host and the virtual machine is powered off.

1. If it is not already running, launch a local console.

   Start > Programs > VMware > VMware GSX Server

2. Open the virtual machine in which you want to use the generic SCSI device. Make sure the virtual machine is powered off.
3. From the GSX Server console window, choose Settings > Configuration Editor. The Configuration Editor opens.
4. Click Add to start the Add Hardware Wizard. Click Next.
5. Select the name of the physical device you want to use.

   Then select the virtual device node where you want this device to appear in the virtual machine.

   The check box at the top of the wizard screen allows you to specify whether the device should be connected each time the virtual machine is powered on.
6. Click Finish to install the new device.

To remove this device, launch the Configuration Editor, select the generic SCSI device, then click Remove.

Generic SCSI on a Linux Host Operating System

Using the SCSI Generic driver in Linux, GSX Server allows your guest operating system to operate generic SCSI devices within a virtual machine. The SCSI Generic driver sets up a mapping for each SCSI device in `/dev`. Each entry starts with `sg` (for the SCSI Generic driver) followed by a letter. For example, `/dev/sga` is the first generic SCSI device.

Each entry corresponds to a SCSI device, in the order specified in `/proc/scsi/scsi`, from the lowest device ID on the lowest adapter to the highest device ID on the lowest adapter, and so on to the highest device ID on the highest adapter. Do not enter `/dev/st0` or `/dev/scd0`.

Note: When setting up a generic SCSI device in the Configuration Editor, as described later in this section, you specify the device you wish to install in the virtual machine by typing its `/dev/sg` entry in the name field.

Requirements

Generic SCSI requires version 2.1.36 of the SCSI Generic (`sg.o`) driver, which comes with kernel 2.2.14 and higher.

Avoiding Concurrent Access to a Generic SCSI Device

Under Linux some devices — specifically tape drives, disk drives and CD-ROM drives — already have a designated `/dev` entry (traditionally, `st`, `sd` and `scd`, respectively). When the SCSI Generic driver is installed, Linux also identifies these devices with an `sg` entry in `/dev` — in addition to their traditional entries. GSX Server ensures that multiple programs are not using the same `/dev/sg` entry at the same time but cannot always ensure that multiple programs are not using the `/dev/sg` and the traditional `/dev` entry at the same time. It is important that you do not attempt to use the same device in both host and guest. This can cause unexpected behavior and may cause loss or corruption of data.

Permissions on a Generic SCSI Device

You must have read and write permissions on a given generic SCSI device in order to use the device within a virtual machine, even if the device is a read-only device such as a CD-ROM drive. These devices typically default to root-only permissions. Your administrator should create a group with access to read and write to these devices and then add the appropriate users to that group.

Adding a Generic SCSI Device to a Virtual Machine

You can add generic SCSI devices to your virtual machine in the Configuration Editor. The Configuration Editor lets you map virtual SCSI devices to physical generic SCSI devices on the host.

When you set up a generic SCSI device, the virtual machine must be powered off.

1. Launch a local console (`vmware -G`) and select the virtual machine. Make sure the virtual machine is powered off.
2. Choose **Settings** > **Configuration Editor**. The Configuration Editor opens.
3. Click the + sign next to **SCSI devices**. The list of this virtual machine's SCSI devices appears.
4. Select an unassigned SCSI device where the generic SCSI device is to be installed. At this time, this device is labeled **Not Installed**. Now you can specify the characteristics of the virtual SCSI device.
5. In the **Device Type** list, select **Generic Device**.
6. In the **Name** field, enter the name of the `/dev/sg` entry for the device you want to install in the virtual machine. For example, if this device is named `sga`, type `/dev/sga` in the **Name** field.
7. Click **Install**.
8. Click **OK** to save the configuration and close the Configuration Editor.

To remove this device, launch the Configuration Editor, select the generic SCSI device, then click **Remove**.

15

Performance Tuning

Adjusting Virtual Machines for Best Performance

The following sections offer suggestions for getting the best performance from VMware GSX Server and your virtual machines:

- Configuring GSX Server on page 523
  - General GSX Server Options on page 523
  - GSX Server on a Windows Host on page 527
  - GSX Server on a Linux Host on page 528
- Understanding Memory on page 529
  - Virtual Machine Memory Size on page 529
  - Reserved Memory on page 530
  - Using More than 1GB of Memory on a Linux 2.2.x Kernel Host on page 532
- Improving Performance for Guest Operating Systems on page 534
  - Windows 2000, Windows XP and Windows Server 2003 Guest Operating System Performance Tips on page 534
  - Windows 95 and Windows 98 Guest Operating System Performance Tips on page 536
  - Linux Guest Operating System Performance Tips on page 538

Configuring GSX Server

This section offers advice and information about factors that can affect the performance of GSX Server itself. This section does not address performance of the guest operating system or the host operating system.

Note: In addition to the GSX Server configuration options discussed below, you should always install VMware Tools in any guest operating system for which a VMware Tools package exists. Installing VMware Tools provides better video and mouse performance and also greatly improves the usability of the virtual machine. For details, see Installing VMware Tools on page 113.

General GSX Server Options

Guest Operating System Selection

Make certain you select the correct guest operating system for each of your virtual machines. To check the guest operating system setting, choose **Settings** > **Configuration Editor** > **Options** (on a Windows host) or **Settings** > **Configuration Editor** > **Misc** (on a Linux host).

GSX Server optimizes certain internal configurations on the basis of this selection. For this reason, it is important to set the guest operating correctly. The optimizations can greatly aid the operating system they target, but they may cause significant performance degradation if there is a mismatch between the selection and the operating system actually running in the virtual machine. (Selecting the wrong guest operating system should not cause a virtual machine to run incorrectly, but it may degrade the virtual machine's performance.)

Memory Settings

Make sure to choose a reasonable amount of memory for your virtual machine. Many modern operating systems are increasingly hungry for memory, so assigning a healthy amount is a good thing.

The same holds true of the host operating system, especially a Windows host.

The New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) automatically selects a reasonable starting point for the virtual machine's memory, but you may be able to improve performance by adjusting the settings during installation or later in the Configuration Editor (**Settings** > **Configuration Editor** > **Memory**).

If you plan to run one virtual machine at a time most of the time, a good starting point is to give the virtual machine half the memory available on the host.

Adjusting the reserved memory settings may also help. In the local console on a Windows host, go to **Settings** > **Preferences** > **Memory**. In the local console on a Linux host, go to **Settings** > **Reserved Memory**.

For additional information, see Understanding Memory on page 529.

Debugging Mode

GSX Server can run in two modes — normal mode and a mode that provides extra debugging information. The debugging mode is slower than normal mode.

For normal use, check to be sure you aren't running in debugging mode. On a Windows host, choose **Settings** > **Configuration Editor** > **Advanced** and make sure **Run with debugging information** is not checked**.** On a Linux host, choose **Settings** > **Configuration Editor** > **Misc** and make sure the **Run with debugging information** option is not selected.

CD-ROM Drive Polling

Some operating systems — including Windows NT and Windows 98 — poll the CD-ROM drive every second or so to see whether a disc is present. (This allows them to run autorun programs.) This polling can cause GSX Server to connect to the host CD-ROM drive, which can make it spin up while the virtual machine appears to pause.

If you have a CD-ROM drive that takes especially long to spin up, there are two ways you can eliminate these pauses.

- You can disable the polling inside your guest operating system. The method varies by operating system. For recent Microsoft Windows operating systems, the easiest way is to use TweakUI from the PowerToys utilities.

  For information on finding TweakUI and installing it in your guest operating system, go to *www.microsoft.com* and search for TweakUI. Specific instructions depend on your operating system.

- Another approach is to configure your virtual CD-ROM drive to start disconnected. The drive appears in the virtual machine, but it always appears to contain no disc (and GSX Server does not connect to your host CD-ROM drive).

  To make this change, go to **Settings** > **Configuration Editor**. On a Windows host, click the DVD/CD-ROM item in the **Device** list. On a Linux host, expand either **IDE Drives** or **SCSI Drives** (depending on how you have configured your virtual CD-ROM drive) and click the device that represents your virtual CD-ROM drive.

Then clear the **Connect at Power On** check box (on a Windows host) or **Start Connected** check box (on a Linux host).

When you want to use a CD-ROM in the virtual machine, go to the **Devices** menu and connect the CD-ROM drive.

Disk Options

The various disk options (SCSI versus IDE) and types (virtual or raw) affect performance in a number of ways.

Inside a virtual machine, SCSI disks and IDE disks that use direct memory access (DMA) have approximately the same performance. However, IDE disks can be very slow in a guest operating system that either cannot use or is not set to use DMA.

The easiest way to configure a Linux guest to use DMA for IDE drive access is to install VMware Tools (**Settings** > **VMware Tools Install**). Among other things, the installation process automatically sets IDE virtual drives to use DMA.

In Windows Server 2003, Windows XP and Windows 2000, DMA access is enabled by default. In other Windows guest operating systems, the method for changing the setting varies with the operating system. See the following technical notes for details.

- Disk Performance in Windows NT Guests on Multiprocessor Hosts on page 402
- Windows 95 and Windows 98 Guest Operating System Performance Tips on page 536

Virtual disks in nonpersistent and undoable mode often have very good performance for random or nonsequential access. But they can potentially become fragmented to a level that cannot be fixed with defragmentation tools inside the guest. This can slow performance.

When run in persistent mode, raw disks and plain disks both use flat files that mimic the sequential and random access performance of the underlying disk. When you are using undoable mode and have made changes since powering on the virtual machine, any access to those changed files performs at a level similar to the performance of a virtual disk. Once you commit the changes, performance is again similar to that of the underlying disk.

Overall, if you are using raw (or plain) disks in persistent mode, you see somewhat better performance than that provided by other disk types and modes.

In exchange, because you are using persistent mode, you sacrifice the ability to undo the writing of any information to the disk. And because you are not using virtual disks, you cannot take advantage of the fact that virtual disks initially have a small footprint in the host file system and grow only as needed as you fill the virtual disk.

Remote Disk Access

Whenever possible, do not use disks that are on remote machines and accessed over the network unless you have a very fast network. If you must run disks remotely, make certain to use disks in undoable mode. Then go to **Settings** > **Configuration Editor** > **Options** (on Windows hosts) or **Settings** > **Configuration Editor** > **Misc** (on Linux hosts) and set the **Redo Log Directory** to a directory on your local hard disk.

Issues Installing or Running Applications in a Guest Operating System

You may notice that whenever you try to install or start a particular program in a virtual machine, the program seems to hang, crash or complain that it is running under a debugger. VMware has seen this problem with a few programs, including the installer for the Japanese version of Trend Micro Virus Buster, the FoxPro database, the NetWare client in Windows 98, Mathcad, The Sims and Civilization III.

You can work around this problem by using a special setting called disabling acceleration. Frequently, the problem occurs only during installation or early in the program's execution; in that case you should turn acceleration back on after getting past the problem. Follow these steps:

1. Power on the virtual machine.
2. Before running or installing the program that was encountering problems, disable acceleration.

   On a Windows host, choose **Settings** > **Configuration Editor** > **Advanced** and check the **Disable acceleration** check box.

   On a Linux host, choose **Settings** > **Configuration Editor** > **Misc** and check the **Disable acceleration** check box.
3. Click **OK** to save the change and close the Configuration Editor.
4. Start the program or run the installer.
5. After you pass the point where the program was encountering problems, return to the Configuration Editor and remove the check beside **Disable acceleration**. You may be able to run the program with acceleration after it is started or installed.

   Note: Disabling acceleration can help you get past the execution problem, but it causes the virtual machine to run slowly. If the problem occurs only at startup or during installation, you can improve performance by resuming accelerated operation after the program that was encountering problems is running or is installed.

GSX Server on a Windows Host

Note: The items in this section describe performance of GSX Server on a Windows host. For tips on configuring GSX Server on a Linux host, see GSX Server on a Linux Host on page 528.

Process Scheduling

Note: The information in this hint was created to address scheduling problems with Windows NT. The issues are likely to be different in Windows 2000 and Windows Server 2003; however, we do not currently have corresponding information for Windows 2000 or Windows Server 2003 hosts.

The process scheduler on Windows NT does not necessarily schedule processes in a way that allows you to get the best performance from your particular combination of virtual machines and applications running on the host. GSX Server on a Windows host has configuration options that let you adjust scheduling priorities to meet your needs.

These configuration options are available from the **Settings** > **Preferences** > **Priority** tab. They allow you to specify either high or normal priority when the mouse and keyboard are grabbed by the virtual machine and either normal or low priority when they are not grabbed.

Your selection under **Global Preference** is taken as the default across all virtual machines. Your selection under **Local Setting** overrides the global settings for just the specific virtual machine where you make the changes.

Pay particular attention to the **grabbed: HIGH – ungrabbed: NORMAL** and **grabbed: NORMAL – ungrabbed: LOW** settings.

The **grabbed: HIGH – ungrabbed: NORMAL** setting is useful if you have many background processes or applications and you do not care if they run with fairly low relative priority while GSX Server is in the foreground. In return, you get a very noticeable performance boost using a GSX Server virtual machine while another virtual machine is running or while some other processor-intensive task (a compile, for example) is running in the background.

The reverse is true of the **grabbed: NORMAL – ungrabbed: LOW** setting. If your host machine feels too sluggish when a virtual machine is running in the background, you can direct the virtual machine to drop its priority when it does not have control of the mouse and keyboard. As with the high setting, this is a heavy-handed priority change, so the virtual machine and any background applications run much more slowly.

GSX Server on a Linux Host

Note: The items in this section describe performance of GSX Server on a Linux host. For tips on configuring GSX Server on a Windows host, see GSX Server on a Windows Host on page 527.

Using Full Screen Mode

Full screen mode is faster than window mode. As a result, if you do not need to have your virtual machine and your host sharing the screen, try switching to full screen mode. You can use full screen mode only when the virtual machine is running in a local console.

Note: The extreme case of this is VGA mode. VGA mode is any mode in which the screen is in text mode (DOS, for example, or Linux virtual terminals), or 16-color 640 x 480 graphics mode (for example, the Windows 9x clouds boot screen or any guest operating system that is running without the SVGA driver provided by VMware Tools).

On a Linux host, full screen VGA mode uses the underlying video card directly, so graphics performance is effectively very close to that of the host. By contrast, window mode VGA is more expensive to emulate than window mode SVGA. As a result, if you need to run for an extended period of time in VGA mode (for example, when you are installing an operating system using a graphical installer) you should see a very significant performance boost if you run in full screen mode.

System Timer

Certain guests (Windows 98, for example) expect a very high interrupt rate from their system timers. GSX Server on a Linux host uses `/dev/rtc`, the real-time clock device, to try to keep up. However, continually servicing `/dev/rtc` and using it to maintain a high interrupt rate increases the load on the host, even when the virtual machine does not appear to be busy.

To try running without `/dev/rtc`, disconnect it using the **Devices** menu in a console. This may not make a critical difference in performance, but it can help reduce the load on the host.

Understanding Memory

GSX Server allows users to set the memory size of each virtual machine and the amount of physical host memory reserved for virtual machines. By adjusting the memory sizes of each virtual machine and the amount of reserved memory, users can affect both virtual machine and overall system performance. The following sections describe how GSX Server uses the memory configuration parameters to properly manage virtual machines and reserved memory.

Virtual Machine Memory Size

The first configuration parameter users can set is the size of the virtual machine's physical memory. This configuration parameter can be set via the Configuration Editor (**Settings** > **Configuration Editor** > **Memory**). The minimum size of the memory for the virtual machine should be set based on the recommendations of the operating system provider.

The New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) sets what VMware believes are reasonable defaults for the memory size of a virtual machine based on the type of the guest operating system and the amount of memory in the host computer.

The actual size that should be given to a virtual machine depends on a few practical considerations:

- What kinds of applications are to be run in the virtual machine
- What other virtual machines will be contending with this virtual machine for memory resources
- What applications are going to be running on the host at the same time as the virtual machine

Windows operating systems do not behave well when they run low on free memory. For this reason users should not run virtual machines whose memory requirements exceed that of the host and other applications. To help guard against virtual machines causing the host to thrash, GSX Server enforces a limit on the total amount of memory that may be consumed by virtual machines:

The sum of the memories of all currently running virtual machines plus overhead for the GSX Server processes cannot exceed the amount of physical memory on the host minus some memory that must be kept available for the host.

Some memory must be kept available on the host to ensure the host is able to operate properly while virtual machines are running. The amount of memory reserved for the host depends on the host and the size of the host's memory.

If you want the most memory out of your virtual machine and are pushing close to the supported limits, you should expect that if you run the virtual machine for a while, power it off and change settings in the Configuration Editor (especially increasing the virtual machine's memory size), then try to power it back on, the virtual machine may not power on. If this happens, close the console in which you tried opening the virtual machine, and open a new console. The virtual machine should power on.

Reserved Memory

The second configuration parameter that users can set is the amount of memory that GSX Server is allowed to reserve for all running virtual machines. This parameter can be set in **Settings** > **Preferences** > **Memory** (on Windows hosts) or **Settings** > **Reserved Memory** (on Linux hosts).

This setting specifies a maximum amount that GSX Server is allowed to reserve. But this memory is not allocated in advance. Even if multiple virtual machines are running at the same time, however, GSX Server may be using only a fraction of the reserved memory. Any unused reserved memory is available to be used by other applications. If all the reserved memory is in use by one or more virtual machines, the host operating system cannot use this memory itself or allow other applications to use it.

The memory used by GSX Server includes the memory made available to the guest operating systems plus a small amount of overhead memory associated with running a virtual machine. The amount of overhead memory required depends upon the size of the guest's virtual disks, its behavior and the amount of memory allocated to the virtual machine. Refer to the table below for the typical upper limit needed, based on the amount of memory allocated to the guest.

Amount of Memory Allocated to the Virtual Machine	Additional Amount of Overhead Needed
Up to 512MB	Up to 40MB
Up to 1GB	Up to 50MB
Up to 2GB	Up to 70MB

The amount of memory actually used for a particular virtual machine varies dynamically as a virtual machine runs. If multiple virtual machines run simultaneously, they work together to manage the reserved memory.

The recommended amount of memory to reserve for all running virtual machines is calculated on the basis of the host computer's physical memory and is displayed in the reserved memory settings control — **Settings** > **Preferences** > **Memory** (on Windows hosts) or **Settings** > **Reserved Memory** (on Linux hosts). If you determine you want GSX Server to reserve more or less physical memory, you can use this control to change the amount.

Reserving too much physical memory can cause the host to thrash, or even hang, if other applications are run on the host. Reserving too little physical memory can cause virtual machines to perform very poorly and also limit the number of virtual machines that can be run.

Limits on the Number of Running Virtual Machines

By default, GSX Server limits the number of virtual machines that can run at once based on the amount of reserved memory. This prevents virtual machines from causing each other to perform very poorly. If you try to power on a virtual machine when there is insufficient reserved memory available, it fails to power on.

You can change the memory check so it only displays a warning message, rather than preventing the virtual machine from powering on. To do so, go to **Settings** > **Preferences** > **Memory** (on Windows hosts) or **Settings** > **Reserved Memory** (on Linux hosts) and clear the **Enable Memory Limits** check box.

Disabling Memory Checks for Virtual Machines

By default, virtual machines perform checks to ensure that the amount of memory allocated to running virtual machines plus an overhead does not exceed the limits imposed by the user or by GSX Server defaults.

If you need to allocate more memory to your virtual machines, you can disable the memory checks (also called memory limits) and change the memory limits. When you disable the memory checks, you:

- Allow a virtual machine to run even though it is configured to run with more memory than is currently available on the host
- Allow a virtual machine to exceed the amount of memory allocated to all running virtual machines

Caution: Disabling the memory limits check can result in poor performance for both the host operating system and guest operating systems. Disabling memory checks can also result in system crashes, low memory warnings or processes in the host abnormally terminating.

To disable memory checks, complete the following steps.

1. On a Windows host, in a local console, select **Settings** > **Preferences**, then click the **Memory** tab.

   On a Linux host, in a local console, select **Settings** > **Reserved Memory**.

2. If you want to allow virtual machines to exceed the amount of memory reserved for them, deselect **Enable memory limits**.

3. Click **OK**.

Using More than 1GB of Memory on a Linux 2.2.x Kernel Host

By default, Linux kernels in the 2.2.x series support 1GB of physical memory. If you want to use more memory on a Linux host with a kernel in the 2.2.x series, you can take one of several approaches.

- Upgrade to a 2.4.x series kernel that allows for more physical memory.
- Recompile your kernel as a 2GB kernel using the CONFIG_2GB option.
- Enable the CONFIG_BIGMEM option to map more physical memory. (This approach requires you to complete specific steps, described in detail in the Workarounds section below; otherwise, GSX Server cannot work on such a kernel.)

The CONFIG_2GB option calls for recompiling your kernel as a 2GB kernel. You do this by recompiling your kernel with CONFIG_2GB enabled. This allows Linux to support nearly 2GB of physical memory by dividing the address space into a 2GB user chunk and 2GB kernel chunk (as opposed to the normal 3GB user and 1GB kernel).

The third approach uses the CONFIG_BIGMEM option in Linux. With the CONFIG_BIGMEM option enabled, the kernel does not directly address all of physical memory and it can then map 1GB (or 2GB) of physical memory into the address space at a time. This allows the use of all of physical memory at the cost of changing the semantics the kernel uses to map virtual to physical addresses. However, VMware products expect physical memory to be mapped directly in the kernel's address space and thus do not work properly with the CONFIG_BIGMEM option enabled.

Workarounds

If you are using a 1GB kernel with CONFIG_BIGMEM enabled and have 960MB to 1983MB of memory, GSX Server does not run. To work around this issue, you can try one of the following:

- Recompile the kernel as a 2GB kernel by enabling the CONFIG_2GB option. This allows for 100 percent use of physical memory.

- Pass the boot-time switch `mem=959M` at the LILO prompt, or add it to `lilo.conf`, to disable CONFIG_BIGMEM and thus allow you to run GSX Server. To do this:
  - At the LILO prompt, type `linux-2.2.16xxx mem=959M`.
  - Or, edit `lilo.conf`. In the kernel section, add this line:
    `append mem="959M"`

If you have a 1GB kernel with CONFIG_BIGMEM enabled and have more than 1983MB of memory, you can do one of the following:

- Recompile the kernel as a 2GB kernel by enabling the CONFIG_2GB option and either pass the boot-time switch `mem=1983M` at the LILO prompt or add it to `lilo.conf`. To use the switch:
  - At the LILO prompt, type `linux-2.2.16xxx mem=1983M`.
  - Or, edit `lilo.conf`. In the kernel section, add this line:
    `append mem="1983M"`
- Pass the boot-time switch `mem=959M` at the LILO prompt or add it to `lilo.conf` to disable CONFIG_BIGMEM. To use the switch:
  - At the LILO prompt, type `linux-2.2.16xxx mem=959M`.
  - Or, edit lilo.conf. In the kernel section, add this line:
    `append mem="959M"`

If you are using a 2GB kernel with CONFIG_BIGMEM enabled and have 1984MB or more memory, GSX Server does not run. You can either pass the boot-time switch `mem=1983M` at the LILO prompt, or add it to `lilo.conf`, to disable CONFIG_BIGMEM and thus allow you to run GSX Server. To use the switch:

- At the LILO prompt, type `linux-2.2.16xxx mem=1983M`.
- Or, edit `lilo.conf`. In the kernel section, add this line:
  `append mem="1983M"`

Improving Performance for Guest Operating Systems

The tips in this section help you make adjustments to improve performance for particular guest operating systems running inside a virtual machine.

Windows 2000, Windows XP and Windows Server 2003 Guest Operating System Performance Tips

This section offers advice for configuring a Windows 2000, Windows XP or Windows Server 2003 guest operating system for better performance inside a virtual machine.

Note: This section pertains to the guest operating system that is running inside a GSX Server virtual machine. It does not describe actions that should be taken on the Windows 2000 or Windows Server 2003 host operating system.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the Configuration Editor — **Settings** > **Configuration Editor** > **Options** (on Windows hosts) or **Settings** > **Configuration Editor** > **Misc** (on Linux hosts).

VMware Tools

Make certain VMware Tools is installed. VMware Tools provides an optimized SVGA driver and sets up the VMware Tools service to run automatically when the system starts. Among other things, the VMware Tools service allows you to synchronize the virtual machine's clock with the host computer's clock, which can improve performance for some functions. You can install VMware Tools by choosing **Settings** > **VMware Tools Install**.

Disconnect CD-ROM, /dev/rtc

Using the **Devices** menu, disconnect your CD-ROM drive if you do not need to use it. If you are using a Linux host, also disconnect `/dev/rtc`. Disconnecting these devices reduces CPU usage.

Note: The time synchronization feature in VMware Tools does not rely on `/dev/rtc`.

Visual Effects

The fade effects that Windows 2000, Windows XP and Windows Server 2003 use when displaying menus can be somewhat slow and make the virtual machine seem less responsive.

To disable them, right-click the guest operating system desktop, then choose **Properties** > **Appearance** > **Effects** (on Windows XP or Windows Server 2003) or **Properties** > **Effects** (on Windows 2000) and uncheck **Use transition effects for menus and tool tips**.

Full Screen Mode

Run your virtual machine in full screen mode. Click the **Full Screen** button on the local console toolbar. You can use full screen mode only when the virtual machine is running in a local console.

Enabling Hardware Acceleration (Windows Server 2003 Guests Only)

Prerelease versions of Windows Server 2003 have hardware acceleration disabled by default. This slows down graphics performance and mouse responsiveness in the guest operating system.

To enable hardware acceleration in a Windows Server 2003 guest, open the Control Panel, then open the Display Properties control panel. On the **Settings** tab, click **Advanced**. On the **Troubleshoot** tab, drag the **Hardware acceleration** slider all the way to **Full**.

Windows 95 and Windows 98 Guest Operating System Performance Tips

This section offers advice for configuring a Windows 95 or Windows 98 guest operating system for better performance inside a GSX Server virtual machine.

Note: This section pertains to the guest operating system that is running inside a virtual machine. It does not describe actions that should be taken on a client.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the Configuration Editor — Settings > Configuration Editor > Options (on Windows hosts) or Settings > Configuration Editor > Misc (on Linux hosts).

VMware Tools

Make certain VMware Tools is installed. VMware Tools provides an optimized SVGA driver and sets up the VMware Tools service to run automatically when the system starts. Among other things, the VMware Tools service allows you to synchronize the virtual machine's clock with the host computer's clock, which can improve performance for some functions. You install VMware Tools by choosing Settings > VMware Tools Install.

DMA Mode for IDE Disks

Windows 95 OSR2 and later (including Windows 98) can use direct memory access (DMA) for faster IDE hard disk access. However, DMA may not be enabled by default.

You can turn on DMA access using the guest operating system's Device Manager.

1. Right-click My Computer and choose Properties from the pop-up menu.
2. Click the + sign beside Disk Drives to show your virtual machine's individual drives.
3. Right-click the entry for each IDE drive to open its properties dialog box.
4. Under Settings, check the DMA box and accept any warning Windows displays.
5. Restart Windows for the new settings to take effect.

Full Screen Mode

Run your virtual machine in full screen mode. Click the Full Screen button on the local console toolbar. You can use full screen mode only when the virtual machine is running in a local console.

Swap File Usage

In your `system.ini` file, in the `[386enh]` section, add the following line:

```
ConservativeSwapFileUsage=1
```

Disconnect CD-ROM and /dev/rtc

Using the **Devices** menu, disconnect your CD-ROM drive if you do not need to use it.

If you are using a Linux host and have a Windows 95 guest, also disconnect `/dev/rtc`. Do not disconnect it in a Windows 98 guest.

Disconnecting these devices reduces CPU usage.

Note: The time synchronization feature in VMware Tools does not rely on `/dev/rtc.`

Visual Effects

Windows 98 has a number of visual effects, designed to be attractive, that place unnecessary demands on the graphics emulation in GSX Server. Some users have seen performance improvements when they turn off these special effects.

To modify these settings, right-click on the desktop of your virtual machine, then select **Properties** from the pop-up menu. Click the **Effects** tab and uncheck the **Animate windows, menus, and lists** check box.

Also, if you have **Show window contents while dragging** checked, try unchecking that check box.

Linux Guest Operating System Performance Tips

This section offers advice for configuring a Linux guest operating system for better performance inside a GSX Server virtual machine.

Note: This document pertains to the guest operating system that is running inside a GSX Server virtual machine. It does not describe actions that should be taken on Linux running on the host.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the Configuration Editor — **Settings** > **Configuration Editor** > **Options** (on Windows hosts) or **Settings** > **Configuration Editor** > **Misc** (on Linux hosts).

VMware Tools

Make certain VMware Tools is installed. VMware Tools provides an optimized SVGA driver and sets up the VMware Tools service to run automatically when the system starts. Among other things, the VMware Tools service allows you to synchronize the virtual machine's clock with the host computer's clock, which can improve performance for some functions. You can install VMware Tools by choosing **Settings** > **VMware Tools Install**.

Disconnect CD-ROM, /dev/rtc

Using the **Devices** menu, disconnect your CD-ROM drive if you do not need to use it. If you are using a Linux host, also disconnect `/dev/rtc`. Disconnecting these devices reduces CPU usage.

Note: The time synchronization feature in VMware Tools does not rely on `/dev/rtc`.

Install in Text Mode

When you are installing your Linux guest operating system, use the text-mode installer instead of the graphical installer if you have a choice. This makes the installation process faster.

If you do use a graphical installer and if you are using a Linux host computer, try to run the virtual machine in a local console in full screen mode during the installation.

Full Screen Mode

Run your virtual machine in full screen mode. Click the **Full Screen** button on the local console toolbar. You can use full screen mode only when the virtual machine is running in a local console.

16

High-Availability Configurations with GSX Server

High-Availability Configurations with VMware GSX Server

This section contains the following:

- Using SCSI Reservation to Share SCSI Disks With Virtual Machines on page 541
- Overview of Clustering with GSX Server, which includes:
  - Applications that Can Use Clustering on page 547
  - Clustering Software in Virtual Machines on page 547
- Clustering Scenario: Cluster in a Box on page 548
- Clustering Scenario: Network Load Balancing with GSX Server on page 557

Using SCSI Reservation to Share SCSI Disks With Virtual Machines

GSX Server permits the sharing of plain disks with multiple virtual machines running on the same host, provided the disk in question is a SCSI disk.

Note: Although virtual and raw disks can be used with SCSI reservation, such use is considered experimental. Only the use of plain disks is fully supported with SCSI reservation. To create a plain disk, see Adding Plain Disks to a Virtual Machine on page 388.

When the disk is shared, all virtual machines connected to the disk are able to write to the disk concurrently with the SCSI reservation protocol.

This feature is advanced and should only be used if you are familiar with SCSI in general and the SCSI reservation protocol in particular.

In addition, clustering software must be installed in each virtual machine that intends to share a SCSI disk. Enabling SCSI reservation in and of itself does not automatically mean that a running virtual machine is a participant in the SCSI reservation protocol.

The following sections describe how to use SCSI reservation to share disks among multiple virtual machines.

- SCSI Reservation Support on page 542
- Enabling SCSI Reservation on page 543
- Issues to Consider When Sharing Disks on page 544

SCSI Reservation Support

SCSI reservation support is limited by the following:

- You can enable SCSI reservation for SCSI virtual, raw and plain disks. No other type of SCSI devices can use SCSI reservation in a virtual machine. Specifically, you **cannot** enable SCSI reservation for a generic SCSI disk. SCSI reservation support for virtual disks is experimental.

  Note: VMware supports SCSI reservation when used with plain disks. Support for SCSI reservation with virtual and raw disks is considered experimental. For high-availability configurations, use SCSI reservation with plain disks.

- SCSI disks can be shared via reservation among virtual machines running on the same host. This means that the configuration files for the virtual machines must all be running on the same GSX Server host. However, the disk or disks the virtual machines are sharing can be located remotely on a different host.
- Even though the virtual or plain disk is a SCSI disk, it can be located on a host running on an IDE drive. A raw disk must always be a SCSI disk.
- GSX Server virtual machines currently support only the SCSI-2 disk protocol, but not applications using SCSI-3 disk reservations. However, all popular clustering software (including MSCS and VCS) currently use SCSI-2 reservations.

Enabling SCSI Reservation

SCSI reservation must be enabled in a virtual machine before you can share its disks. To enable it, make sure the virtual machine is powered off. Open the configuration file (`.vmx` file on Windows hosts, `.cfg` file on Linux hosts) in a text editor and add the line `scsi[n].sharedBus = "virtual"` anywhere in the file, where `[n]` is the SCSI bus being shared.

VMware recommends you set up the shared disks on their own SCSI bus, which is a different bus than the one the guest operating system uses. For example, if your guest operating system is on `scsi0:0`, you should set up disks to share on `scsi1` bus.

For example, to enable SCSI reservation for devices on the `scsi1` bus, add the following line to the virtual machine's configuration file:

```
scsi1.sharedBus = "virtual"
```

This gives the whole bus the ability to be shared. However, if you would rather not share the whole bus, you can selectively enable SCSI reservation for a specific SCSI disk on the shared bus. This prevents the locking of this specific disk. Add the following line to the configuration file:

```
scsi1:1.shared = "true"
```

If SCSI reservation is enabled (that is, `scsi1.sharedBus` is set to `"virtual"`), then this setting is ignored.

In addition to enabling SCSI reservation on the bus, you need to allow virtual machines to access the shared disk concurrently. Add the following line to the virtual machine's configuration file:

```
disk.locking = "false"
```

This setting permits multiple virtual machines to access a disk concurrently. Be careful though; if any virtual machine not configured for SCSI reservation tries to access this disk concurrently, then the shared disk is vulnerable to corruption or data loss.

When SCSI reservation is enabled, a reservation lock file that contains the shared state of the reservation for the given disk is created. The name of this file consists of the filename of the SCSI disk appended with `.RESLCK`.

For example, if the disk `scsi1:0.filename` is defined in the configuration file as

```
scsi1:0.fileName = "/<path_to_config>/vmSCSI.pln"
```

then the reservation lock file for this disk is given the default name

```
"/<path_to_config>/vmSCSI.pln.RESLCK"
```

However, you can provide your own lock file name. Add a definition for `scsi1:0.reslckname` to the configuration file. For example, if

```
scsi1:0.reslckname = "/tmp/scsi1-0.reslock"
```

is added to the configuration file, it overrides the default lock file name.

Selecting the Disk

Once SCSI reservation is enabled for a disk — that is, the `scsi[n].sharedBus = "virtual"` and `disk.locking = "false"` settings are added to the configuration file for each virtual machine wanting to share this disk, you need to point to this disk for each virtual machine that wants to access it.

Sharing a Disk on the scsi0 Bus

VMware does not recommend sharing a disk on SCSI bus 0.

Issues to Consider When Sharing Disks

- Do **not** try to share a disk among multiple running virtual machines that are not collocated on the **same** host. The disk file itself may be located remotely, but the virtual machines must be running together on the same GSX Server host. If you try to share a disk among virtual machines located on different hosts, you could encounter the same unpredictable results you would expect to find if you disabled disk locking.
- If only one running virtual machine is using a given disk, and it is running applications that do not use SCSI reservation, then the disk's performance might be degraded slightly.
- At this time, if one virtual machine does **not** have SCSI reservation enabled for its virtual disk, but another virtual machine **does** have SCSI reservation enabled for the same virtual disk, GSX Server **does** allow the disk to be shared. However, any virtual machine not configured for SCSI reservation that tries to access this disk concurrently can cause corruption or data loss on the shared disk. VMware recommends you take care when sharing disks.
- If you need to shrink or defragment the virtual disk, first disable SCSI reservations and make sure it is not being used by any other virtual machine. To disable SCSI reservation for a virtual machine, open the configuration file and comment out or remove the `scsi[n].sharedBus = "virtual"` line and setting `disk.locking = "true"`.
- If your host abnormally terminates or another action occurs that may require you to repair the plain disk, the virtual machine using the plain disk should be powered on and the disk repaired in one virtual machine before it is used in

another virtual machine. This ensures that only one copy of the disk checker runs at one time.

- On a Windows host, some disk errors are recorded in the Windows event log in normal operation. These error messages have a format similar to:
  `"The driver detected a controller error on \Device\Scsi\BusLogic3"`

  They should be reported periodically only on the passive node of the cluster and should also be reported when the passive node is taking over during a failover. The errors are reported because the active node of the cluster has reserved the shared virtual disk.The passive node periodically probes the shared disk and receives a SCSI reservation conflict error.

Overview of Clustering with GSX Server

GSX Server clustering capabilities are ideally suited for development, testing and training applications.

Note: Always rigorously test and review your cluster before deploying it in a production environment.

This section includes:

- Applications that Can Use Clustering on page 547
- Clustering Software in Virtual Machines on page 547

Clustering is providing a service via a group of servers to get high availability, scalability or both.

For example:

- In a Web server cluster, where the Web site serves static content, a gateway distributes requests to all nodes according to load. The gateway also redirects requests to remaining nodes if one crashes.

  This configuration increases availability and performance over a single-machine approach. Network Load Balancing in Windows 2000 provides such a service.

- In a more complex cluster, a single mode might serve a database. If that node crashes, it must restart the database on another node. The database application knows how to recover from a crash. In normal operation, other nodes run other applications.

  Microsoft Cluster Service and Veritas Cluster Service provide such a service.

In a typical virtual machine cluster

- Each virtual machine is one *node* in the cluster.
- Disks are shared between nodes.
  - These are needed if the application uses dynamic data as mail servers or database servers do.
  - When using virtual disks, they must be plain disks; see Adding Plain Disks to a Virtual Machine on page 388.
- There are extra network connections between nodes for monitoring heartbeat status.
- There is a method for redirecting incoming requests.

Applications that Can Use Clustering

To take advantage of clustering services, applications need to be clustering aware.

Such applications can be

- Stateless, such as Web servers and VPN servers
- With built-in recovery features, like those in database servers, mail servers, file servers or print servers

Clustering Software in Virtual Machines

Available clustering software includes:

- Microsoft Clustering Service (MSCS)

  Provides fail-over support for 2 to 4-node clusters for applications such as databases, file servers and mail servers
- Microsoft Network Load Balancing (NLB).

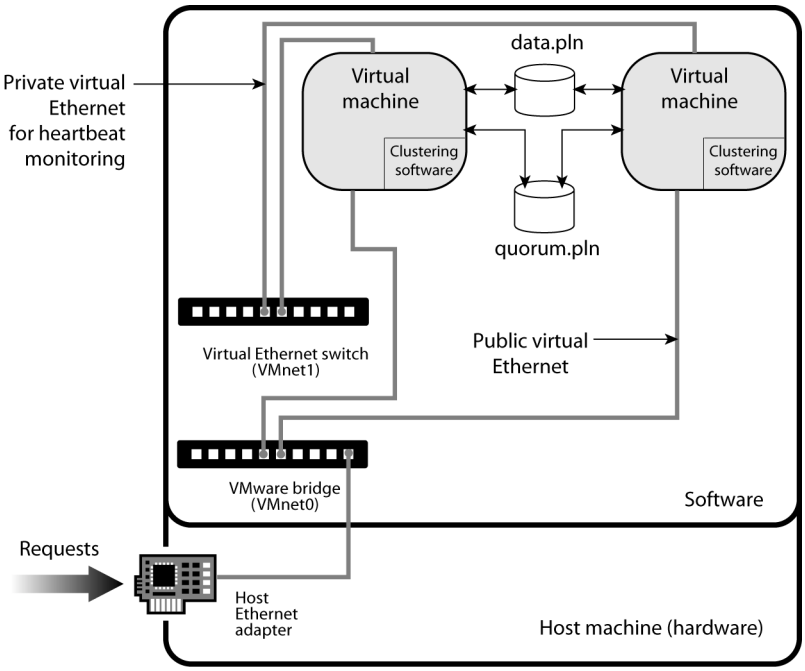
  Load balances incoming IP traffic across a cluster of up to 32 nodes for applications such as Web servers and terminal services.
- Veritas Clustering Service (VCS)

Clustering Scenario: Cluster in a Box

With GSX Server, you can create a simple cluster in a box to help mitigate the effects of software crashes or administrative problems.

This type of cluster

- Consists of multiple virtual machines (nodes) on a single physical machine
- Supports shared disks without any shared SCSI hardware
- Supports a heartbeat network without an extra network adapter



A two-node cluster on a single physical machine.

The following sections describe how to set up a cluster in a box:

- Configuring Virtual Machines for Cluster in a Box on page 549
- Creating a Two-Node Cluster with Microsoft Clustering Services on a Single GSX Server Computer on page 550, which includes:

- Creating the First Node's Base Virtual Machine on page 550
- Installing the Guest Operating System In the First Virtual Machine (Node) on page 552
- Cloning the First Cluster Node on page 552
- Creating the Second Node in the Cluster from the Clone of the First Node on page 553
- Installing Microsoft Clustering Services On the Cluster Nodes on page 554

Configuring Virtual Machines for Cluster in a Box

To create a set of clustered virtual machines (a cluster in a box), configure each of them with the following:

- A primary virtual SCSI host adapter with one SCSI virtual disk
- Two virtual network adapters:
  - A public network adapter bridged to a physical adapter either using VMnet0, or VMnet2-8 as configured in the Configuration Editor of the GSX Server machine
  - A private network adapter connected to VMnet1 (host-only), or another physical adapter (VMnet2 through VMnet8).

    This is the network adapter that the clustering service uses to monitor the heartbeat between nodes.

    This device selection must match in all virtual machines in a cluster set.
- The remaining default virtual machine devices (such as the CD-ROM drive and the floppy disk drive).

In addition to the above devices, the following are required for shared storage:

- A secondary virtual SCSI host adapter
- One or more plain disks that will be shared, attached to the secondary SCSI host adapter

Please note the following about virtual PCI slots in the virtual machines:

- Each virtual machine by default has five PCI slots available.
- In this configuration (two network adapters and two SCSI host bus adapters), four of these slots are used.
- This leaves one more PCI slot for a third network adapter if needed.

Creating a Two-Node Cluster with Microsoft Clustering Services on a Single GSX Server Computer

This procedure creates a two-node cluster using Microsoft Clustering Services on a single GSX Server computer using the following:

- SQL1 = host name of node 1 of the cluster
- SQL2 = host name of node 2 of the cluster
- SQLCLUSTER = public host name of the cluster

The procedures to create a two-node cluster are described in the following sections:

- Creating the First Node's Base Virtual Machine on page 550
- Installing the Guest Operating System In the First Virtual Machine (Node) on page 552
- Cloning the First Cluster Node on page 552
- Creating the Second Node in the Cluster from the Clone of the First Node on page 553
- Installing Microsoft Clustering Services On the Cluster Nodes on page 554

Creating the First Node's Base Virtual Machine

The following steps describe how to create the base virtual machine that serves as the first node in the cluster (and as a template for the additional node) as well as the two plain disks that will be shared among the virtual machines in the cluster.

Note: The virtual disks used to store the operating system and clustering software for each virtual machine (node) in the cluster do not have to be plain disks.

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Start the local console and create a new virtual machine (for information on creating a new virtual machine, see Creating a New Virtual Machine on page 84). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), except you should specify
   - Windows 2000 Advanced Server as the **Guest Operating System**.
   - `SQL1` as the **Virtual machine name** (on a Windows host) or **Display name** (on a Linux host).
   - The virtual machine directory as `d:\cluster\SQL1` (on a Windows host) or `/home/cluster/SQL1/` (on a Linux host).
   - `SQL1` as the **Disk file** name (on a Windows host).

Note: On a Linux host, after you create the virtual machine, you must change the names of all the virtual disk files in `/home/cluster/SQL1` to `SQL1.*`.

- Bridged networking for the virtual machine.

3. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
4. Add a new network adapter that uses either another external adapter or the VMnet1 host-only adapter. (For complete isolation from the host, you may also any unused virtual Ethernet switch, typically VMnet2 through VMnet7.) For information, see Adding and Modifying Virtual Network Adapters on page 415.

   This will be used as the virtual private Ethernet connection for heartbeat monitoring.
5. Add the two plain disks that are to be shared:
   - A shared data disk (call it `data.pln`, for example)
   - A shared quorum disk (call it `quorum.pln`, for example) to store transactions before they are committed to the data disk

   For information, see Adding Plain Disks to a Virtual Machine on page 388.
6. Save your changes and close the Configuration Editor.
7. Manually edit the configuration file `/home/cluster/SQL1/SQL1.cfg` or `d:\cluster\SQL1\SQL1.vmx` using a text editor.
8. Add the following line to the bottom of the configuration file:

   ```
   scsi1.sharedBus = virtual
   disk.locking = "false"
   ```

   This enables SCSI reservation, which is described in more detail in the section Using SCSI Reservation to Share SCSI Disks With Virtual Machines on page 541.

You are finished creating the virtual machine for the first node in your cluster. The next step is to install a guest operating system in the virtual machine.

Installing the Guest Operating System In the First Virtual Machine (Node)

Follow these steps to install Windows 2000 Advanced Server in the virtual machine that is the first node of your cluster:

1. Insert the Windows 2000 Advanced Server CD in the CD-ROM drive on the GSX Server host.
2. Connect to the virtual machine with a local or remote console.
3. Log in as the user who created the virtual machine or as root or administrator.
4. Click **Power On**.
5. Install Windows 2000 Advanced Server on the disk connected to `scsi0`.
6. Accept all of the default options during the installation.

   Note: Do not install the clustering services at this time.
7. When the installation is complete, install VMware Tools in the guest operating system. See Installing VMware Tools on page 113.
8. Remove the Windows 2000 Advanced Server CD from the CD-ROM drive on your GSX Server host.

You are finished installing the guest operating system. The next step is to clone the virtual machine. (Later, you create the second cluster node using the clone.)

Cloning the First Cluster Node

Follow these steps to clone the first virtual machine node:

1. Run `sysprep.exe`, which is available on the Windows 2000 CD in the file `\support\tools\deploy.cab` (or from the Microsoft Web site).

   The `sysprep.exe` utility removes the security ID assigned to the guest operating system, resets the machine information and resets the TCP/IP network configuration.
2. Shut down the guest operating system and power off the virtual machine.
3. Create a directory named `SQL2` under the `cluster` directory.
4. Copy the `SQL1*.vmdk` files into this directory.
5. Change the file names to `SQL2*.vmdk`.

You are finished cloning the first node. You are now ready to create the second node in the cluster using the clone.

Creating the Second Node in the Cluster from the Clone of the First Node

Follow these steps to create the second node in the cluster using the clone of the first node:

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Start the local console and create a new virtual machine (for information on creating a new virtual machine, see Creating a New Virtual Machine on page 84). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), except you should specify
   - Windows 2000 Advanced Server as the **Guest Operating System**.
   - `SQL2` as the **Virtual machine name** (on a Windows host) or **Display name** (on a Linux host).
   - The virtual machine directory as `d:\cluster\SQL2` (on a Windows host) or `/home/cluster/SQL2` (on a Linux host).
   - To use an existing virtual disk. Click **Browse** and select `SQL2.vmdk`.
   - Bridged networking for the virtual machine.
3. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
4. Add a new network adapter that uses either another external adapter or the VMnet1 host-only adapter. For information, see Adding and Modifying Virtual Network Adapters on page 415.
5. Add the two plain disks (`quorum.pln` and `data.pln`) you previously created. For information, see Adding Plain Disks to a Virtual Machine on page 388, but this time choose to **Use an existing virtual disk** and browse to `quorum.pln` and `data.pln`.
6. Click **OK** to save your settings and close the Configuration Editor and console.
7. Manually edit the configuration file `d:\cluster\SQL2\SQL2.vmx` (on a Windows host) or `/home/cluster/SQL2/SQL2.cfg` (on a Linux host) using a text editor.
8. Add the following line to the bottom of the configuration file:
   ```
   scsi1.sharedBus = virtual
   disk.locking = "false"
   ```
   This enables SCSI reservation, which is described in more detail in the section Using SCSI Reservation to Share SCSI Disks With Virtual Machines on page 541.
9. Connect to the VMware Management Interface (`http://<hostname>`) and review the Status Monitor page.

The management interface should list both virtual machines and show them powered off.

You are finished creating the second node.

Now that you have virtual machines for both nodes in your two-node cluster, you are ready to install the clustering services software.

Installing Microsoft Clustering Services On the Cluster Nodes

Follow these steps to install Microsoft Clustering Services on the first node of your cluster:

1. Start the node 1 virtual machine.
2. Follow the Windows 2000 Advanced Server mini-setup prompts to enter
   - Advanced Server's serial number
   - The host name (SQL1)
   - The IP addresses of the public and private network adapters

   Note: For the public network adapter, enter an IP address that belongs to the physical network. For the private IP address, you may use an address like 192.168.x.x with a class C subnet mask (255.255.255.0).
3. At the end of the process, Windows automatically reboots.
4. Start the Disk Administrator and change both shared disks to Basic disks.
5. Format both shared virtual disks with NTFS if they are not already formatted.
6. Assign the first shared disk to `Q:` (quorum) and the second disk to `R:`.

   If you have joined this virtual machine to an existing Active Directory domain, skip to step 11.
7. Run `dcpromo.exe` from the command prompt. This starts the Active Directory Wizard.
8. Set up the current machine as a domain controller. For the domain name, use something similar to `vmcluster.domain.com` where `domain.com` is your DNS domain and `vmcluster` is your Active Directory domain.

   This node may be set up as a new domain tree and also a new domain forest, or it may join existing ones.
9. Make sure the DNS server is installed.
10. Set the domain permissions as mixed mode unless you plan otherwise.

11. To add a cluster services account in the domain, go to **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
12. Add a cluster service account named `cluster`:
    - **Enter the user's password**.
    - Check: **User cannot change password**.
    - Check: **Password never expires**.
13. Insert the Windows 2000 Advanced Server CD in the server's CD-ROM drive.
14. Choose **Control Panel** > **Add/Remove Programs**.
15. Select **Add/Remove Windows Components**.
16. Check the **Cluster Service** component.
17. Click **Next** and follow the prompts to install the service.
18. As you configure Cluster Service, choose **Form a New Cluster**.
19. Specify the cluster name: SQLCLUSTER.
20. Specify the cluster service account created in step 12.
21. Specify that both shared disks should be managed by the cluster service.
22. Indicate the shared disk (`Q:`) to be the quorum disk.
23. Specify which network adapter is public and which is private.
24. Specify the cluster IP address. This is the address that will represent the cluster. It must be on the same network as that of the physical Ethernet device.
25. Stop the cluster service on the local node (node 1) so that the second virtual machine (node 2) can access the shared disks.
    - From Cluster Manager, right-click the node name.
    - Select **Stop Cluster Service**.

You are finished installing Microsoft Clustering Services on the first node. The steps to install the software on the second node are similar.

1. Start the node 2 virtual machine.
2. Repeat step 2 and step 3 in the procedure for the first node.
3. Start the Disk Administrator and assign the first shared disk to `Q:` (quorum) and the second disk to `R:`.
4. Start `dcpromo.exe` and add this virtual machine as a domain controller in the same domain created in step 8, or add it to an existing domain.

Note: The setup in node 2 must match the setup in node 1, which you performed in step 8.

5. In the node 1 virtual machine, start the cluster service.
   - From Cluster Manager, right-click the node name.
   - Select **Start Cluster Service.**
6. In the node 2 virtual machine, repeat step 14 through step 24 in Installing Microsoft Clustering Services On the Cluster Nodes on page 554, **with one exception**: In step 18, select **Join a Cluster**.

You are now finished configuring the cluster.

Clustering Scenario: Network Load Balancing with GSX Server

This section covers procedures for creating a multinode Network Load Balancing cluster using nodes running in virtual machines. These virtual machines can be located on one or more GSX Server computers.

The following sections describe how to create an example Network Load Balancing cluster:

- Overview of Network Load Balancing Clusters on page 557
- Creating a Multinode Network Load Balancing Cluster on page 558, which includes:
  - Creating the First Node's Base Virtual Machine on page 558
  - Installing the Guest Operating System in the First Virtual Machine (Node) on page 559
  - Cloning the First Cluster Node on page 559
  - Creating the Additional Nodes in the Network Load Balancing Cluster on page 560
  - Configuring the Network Load Balancing Cluster on page 561

Overview of Network Load Balancing Clusters

Network Load Balancing is a Windows 2000 Advanced Server feature. Using Network Load Balancing to build a server cluster.

- You can enhance the availability of Internet server programs, such as those used on these types of servers:
  - Web
  - Proxy
  - Domain name service (DNS)
  - FTP
  - Virtual private network (VPN)
  - Streaming media servers
  - Terminal services
- You can scale your server's performance.

- You may create the cluster
  - With virtual machines on the same physical server.
  - With virtual machines on multiple physical servers (all running GSX Server).
- You can use Network Load Balancing clusters in unicast or multicast modes.

  If the cluster is operating in unicast mode (the default), ordinary network communication among cluster nodes is not possible unless each cluster node has at least two network adapters.
- Up to 32 nodes can be configured in the cluster.

Creating a Multinode Network Load Balancing Cluster

The next sections describe how to create a multinode Network Load Balancing cluster.

- Creating the First Node's Base Virtual Machine on page 558
- Installing the Guest Operating System in the First Virtual Machine (Node) on page 559
- Cloning the First Cluster Node on page 559
- Creating the Additional Nodes in the Network Load Balancing Cluster on page 560
- Configuring the Network Load Balancing Cluster on page 561

Creating the First Node's Base Virtual Machine

Follow these steps to create a base virtual machine that will become the first node in your Network Load Balancing cluster:

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Start the local console and create a new virtual machine (for information on creating a new virtual machine, see Creating a New Virtual Machine on page 84). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), except you should specify
   - Windows 2000 Advanced Server as the **Guest Operating System**.
   - `NLB1` as the **Virtual machine name** (on a Windows host) or **Display name** (on a Linux host).
   - The virtual machine directory as `d:\cluster\nlb1` (on a Windows host) or `/home/cluster/nlb1/` (on a Linux host).
   - `nlb1` as the **Disk file** name (on a Windows host).

Note: On a Linux host, after you create the virtual machine, you must change the names of all the virtual disk files in `/home/cluster/nlb1` to `nlb1.*`.

- Bridged networking for the virtual machine.

3. Connect to this virtual machine with the VMware Remote Console and choose **Settings** > **Configuration Editor**.
4. Add a second networking device, binding it to another physical NIC or to the host-only network.

You are finished creating the first virtual machine (node) in the cluster. The next step is to install a guest operating system in the virtual machine.

Installing the Guest Operating System in the First Virtual Machine (Node)

Follow these steps to install Windows 2000 Advanced Server in the virtual machine that is the first node in your load balancing cluster:

1. Insert the Windows 2000 Advanced Server CD in the GSX Server computer's CD-ROM drive.
2. Connect to the virtual machine with a local or remote console.
3. Log in using the user account that created the virtual machine or as root or Administrator.
4. Click **Power On**.
5. Install Windows 2000 Advanced Server on the disk connected to `scsi0`.
6. Accept all the default options during the installation. If desired, you may install the applications at this time. Network Load Balancing is installed by default.
7. When the installation is complete, install VMware Tools in the guest operating system. See Installing VMware Tools on page 113.
8. Remove the Windows 2000 Advanced Server CD from the server's CD-ROM drive.

You are finished creating the first cluster node. You may now clone that node for use in creating other nodes.

Cloning the First Cluster Node

Follow these steps to clone the first cluster node for use in creating the other nodes in the cluster, either on the same physical server or on other machines running GSX Server:

1. Run `sysprep.exe`, which is available on the Windows 2000 CD in the file `\support\tools\deploy.cab` or from the Microsoft Web site.

The `sysprep.exe` utility removes the security ID assigned to the guest operating system, resets the machine information and resets the TCP/IP network configuration.

2. Shut down the guest operating system and power off the virtual machine.
3. Create a directory `NLB2` under the cluster directory, either on the local server or on different machines running GSX Server.
4. Copy the `nlb1*.vmdk` files into this directory.
5. Change the file names to `nlb<n>*.vmdk`. (where `n` is the Network Load Balancing node number.

Repeat step 3 through step 5 for each additional node you wish to create, either on the same physical server, or on additional machines running GSX Server. You may configure up to 32 nodes with Network Load Balancing.

When you are finished making clones of the first node, you are ready to create additional nodes from the clones.

Creating the Additional Nodes in the Network Load Balancing Cluster

Follow these steps for each of the additional nodes you wish to create (up to 32 nodes) in the Network Load Balancing Cluster:

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Start the local console and create a new virtual machine (for information on creating a new virtual machine, see Creating a New Virtual Machine on page 84). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), except you should specify
   - Windows 2000 Advanced Server as the **Guest Operating System**.
   - `NLB2` as the **Virtual machine name** (on a Windows host) or **Display name** (on a Linux host).

     Note: For additional nodes, use the name of that node instead of `nlb2`.
   - The virtual machine directory as `d:\VMware\cluster\nlb2` (on a Windows host) or `/home/cluster/nlb2` (on a Linux host).
   - To use an existing virtual disk. Click **Browse** and select `nlb2.vmdk`.
   - Bridged networking for the virtual machine.
3. Connect to this virtual machine with the VMware Remote Console and choose **Settings** > **Configuration Editor**.

4. Add a second networking device, binding it to another physical NIC or to the host-only network. For information, see Adding and Modifying Virtual Network Adapters on page 415.
5. Close the console and connect to the VMware Management Interface (`http://<hostname>`) and review the Status Monitor page.

   The management interface should list both virtual machines and show them powered off.

After you have finished creating the additional nodes, you are ready to configure the cluster.

Configuring the Network Load Balancing Cluster

You can cluster up to 32 nodes using Network Load Balancing.

To configure the cluster, follow these steps for each node that will join the cluster:

1. Connect to the first node virtual machine with the VMware Remote Console.
2. Power on the virtual machine.
3. Follow the Windows 2000 Server mini-setup prompts to enter the following:
   - The Windows 2000 Advanced Server serial number
   - The host name
   - IP addresses for that host
4. At the end of the process, Windows automatically reboots.
5. Log on to the Windows 2000 Advanced Server virtual machine as Administrator.
6. Open **Network and Dial-up Connections**.
7. Right-click the local area connection on which you will install Network Load Balancing and choose **Properties**.

   The Local Area Connection Properties dialog box appears.
8. Under **Components checked are used by this connection**, select the **Network Load Balancing** check box.
9. Click **Properties**.
10. On the **Cluster Parameters** tab, configure cluster operations using these parameters:
    - **Primary IP Address**: This is the address for the cluster as a whole. This is the address that the clients will use to access the cluster.

- **Subnet Mask**: This is the subnet mask of the network to which the above address belongs.
- **Multicast**: Leave this unchecked, unless your virtual machine was configured with a single network adapter.

  Note: All members of the cluster must use the same setting for the **Multicast** option.

Refer to Network Load Balancing online Help for the remaining options.

11. When you finish with the cluster parameters, click **OK** to return to the Local Area Connection Properties dialog box.
12. Click **OK** to return to the Local Area Connection Status dialog box.
13. Right-click the local area connection on which Network Load Balancing is to be installed, and select **Properties**.
14. Click **Internet Protocol (TCP/IP)**, then click **Properties**.
15. Set up TCP/IP for Network Load Balancing.

    For more information and links to procedures for setting up TCP/IP for Network Load Balancing on single and multiple network adapters, see Related Topics in the Network Load Balancing online Help.

    Note: You must add the cluster's primary IP address to the list of IP addresses bound to the adapter.

Repeat these steps on each host to be used in your Network Load Balancing cluster.

17

Glossary

Glossary

***Bridged networking* —** A type of network connection between a virtual machine and the rest of the world. Under bridged networking, a virtual machine appears as an additional computer on the same physical Ethernet network as the host.
See also Custom networking, Host-only networking and Network address translation.

***Configuration* —** See Virtual machine configuration.

***Configuration Editor* —** A point-and-click editor used to view and modify the configuration of a virtual machine. It can be launched from the **Settings** menu.
See also Configuration Wizard, New Virtual Machine Wizard.

***Configuration Wizard* —** On Linux hosts, a point-and-click interface for convenient, easy creation of a virtual machine configuration. You can launch it from the dialog box that appears when you start VMware GSX Server without specifying a configuration file. You can also launch it from the **File** menu. It prompts you for information, suggesting default values in most cases. It creates files that define the virtual machine, including a virtual machine configuration file and (optionally) a virtual disk or raw disk file.
See also Configuration Editor, New Virtual Machine Wizard.

***Console* —** See Local console and Remote console.

***Custom networking* —** Any type of network connection between virtual machines and the host that does not use the default bridged, host-only or network address translation (NAT) networking configurations. For instance, different virtual machines can be connected to the host by separate networks or connected to each other and not to the host. Any network topology is possible.
See also Bridged networking, Host-only networking and Network address translation.

***Disk mode* —** A property of a disk used in a virtual machine that defines its external behavior but is completely invisible to the guest operating system. There are three modes: persistent (changes to the disk are always preserved when the virtual machine is powered off), undoable (changes are preserved at the user's discretion) and nonpersistent (changes are never preserved). Disk modes may be changed from the Configuration Editor. For a detailed explanation of disk modes refer to Disk Modes: Persistent, Undoable and Nonpersistent on page 368.

***Event log* —** A page in the VMware Management Interface that displays the most recent actions or events recorded in a virtual machine.

***Existing partition* —** A partition on a physical disk in the host machine.
See also Raw disk.

Guest operating system — An operating system that runs in a virtual machine. See also Host operating system.

Headless — A program or application that runs in the background without any interface connected to it. A running virtual machine that has no consoles connected to it is running headless.

Host-only networking — A type of network connection between a virtual machine and the host. Under host-only networking, a virtual machine is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network.
See also Bridged networking, Custom networking and Network address translation.

Host machine — The physical computer on which the VMware GSX Server software is installed. It hosts the VMware GSX Server virtual machines.

Host operating system — An operating system that runs on the host machine. See also Guest operating system.

Local console — An interface to a virtual machine that provides exclusive access to a virtual machine, so the configuration can be changed, an operating system can be installed or the virtual machine can be run in full screen mode. The local console only runs on the host machine where the virtual machine is located.
See also Remote Console.

Network address translation (NAT) — A type of network connection that allows you to connect your virtual machines to an external network when you have only one IP address, and that address is used by the host computer. If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.
See also Bridged networking, Custom networking and Host-only networking.

New Virtual Machine Wizard — On Windows hosts, a point-and-click interface for convenient, easy creation of a virtual machine configuration. You can launch it from the local console window or from the **File** menu in a local console. It prompts you for information, suggesting default values in most cases. It creates files that define the virtual machine, including a virtual machine configuration file and (optionally) a virtual disk or raw disk file.
See also Configuration Editor, Configuration Wizard.

Nonpersistent mode — All disk writes issued by software running inside a virtual machine with a disk in nonpersistent mode appear to be written to disk but are in fact discarded after the virtual machine is powered off. As a result, a virtual disk or raw disk in nonpersistent mode is not modified by VMware GSX Server.
See also Persistent mode, Undoable mode

Persistent mode — All disk writes issued by software running inside a virtual machine are immediately and permanently written to a virtual disk in persistent mode. As a result, a virtual disk or raw disk in persistent mode behaves like a conventional disk drive on a physical computer.
See also Nonpersistent mode, Undoable mode

Plain disk — A type of virtual disk where the full capacity of the disk is allocated when you create the disk, provided the space is available on the host.

See also Raw disk, Safe raw disk file, Virtual disk.

Raw disk — A hard disk in a virtual machine that is mapped to a physical disk drive on the host machine. A virtual machine's disk can be stored as a file on the host file system (see Virtual disk) or on a local hard disk. When a virtual machine is configured to use a raw disk, VMware GSX Server directly accesses the local disk or partition as a raw device (not as a file on a file system). It is possible to boot a previously installed operating system on an existing partition within a virtual machine environment. The only limitation is that the existing partition must reside on a local IDE or SCSI drive.
See also Plain disk, Safe raw disk file, Virtual disk.

Redo log — The file that stores the changes made to a disk in undoable or nonpersistent mode. You can permanently apply the changes saved in the redo log to a disk in undoable mode so they become part of the main disk files. For a disk in nonpersistent mode, however, the redo-log file is deleted when you power off or reset the virtual machine without writing any changes to the disk.

Remote console — An interface to a virtual machine that provides non-exclusive access to a virtual machine from both the server on which the virtual machine is running and from workstations connected to that host machine.
See also Local Console.

Repeatable resume — Resume a virtual machine repeatedly from the same point at which it was suspended using the same suspended state file. This feature works only with virtual disks in nonpersistent mode.
See also Resume.

Resume — Return a virtual machine to operation from its suspended state. When you resume a suspended virtual machine, all applications are in the same state they

were when the virtual machine was suspended.
See also Suspend.

Safe raw disk file — A file containing access privilege information that controls a virtual machine's read/write access to partitions on a raw disk. Proper use of this file prevents dual-boot users from accidentally trying to run the host operating system again as a guest or from another guest operating system for which the virtual machine was not configured. Safe raw disk files can also prevent accidental writes to raw disk partitions from badly behaved operating systems or applications. Safe raw disk files can be created by the Configuration Wizard, the New Virtual Machine Wizard or the Configuration Editor.

Shrink — The method to reclaim unused space in a virtual disk. If there is empty space in the disk, shrinking reduces the amount of space the virtual disk occupies on the host drive. Shrinking virtual disks is a convenient way to convert a virtual disk to the new `.vmdk` format supported by VMware GSX Server 2.

Supported partition — A virtual disk partition that VMware Tools can prepare for shrinking, such as one of the drives that comprise the virtual hard disk. You can choose to not prepare certain partitions for shrinking.
See also Shrink.

Suspend — Save the current state of a running virtual machine. To return a suspended virtual machine to operation, use the resume feature.
See also Resume.

Undoable mode — All writes to a disk in undoable mode issued by software running inside a virtual machine appear to be written to the disk but are in fact stored in a temporary file (`.REDO` file) on the host file system while the virtual machine is running. When the virtual machine is powered off, the user is given three choices: (1) permanently apply all changes to the disk; (2) discard the changes, thus restoring the disk to its previous state; or (3) keep the changes, so that further changes made the next time the virtual machine runs can be added to the log.
See also Nonpersistent mode, Persistent mode

Unsupported partition — A virtual disk partition that VMware Tools cannot prepare for shrinking. Unsupported partitions include read-only drive partitions, partitions on remote devices and partitions on removable devices such as floppy drives or CD-ROM drives.
See also Shrink.

Virtual disk — A virtual disk is a set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. When you configure a virtual machine with a virtual disk, you can install a new

operating system into the disk file without the need to repartition a physical disk or reboot the host.
See also Raw disk.

Virtual machine — A virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host machine concurrently.

Virtual machine configuration — The specification of what virtual devices (disks, memory size and so forth) are present in a virtual machine and how they are mapped to host files and devices.

Virtual machine configuration file — A file containing a virtual machine configuration. It is created by the Configuration Wizard, the New Virtual Machine Wizard or the VMware Management Interface. It is used by VMware GSX Server to identify and run a specific virtual machine. This file has a `.vmx` extension on a Windows host and a `.cfg` extension on a Linux host.

Virtual machine list — On Windows hosts, a list in the local console window that shows the names and guest operating systems of virtual machines that have previously been used with VMware GSX Server. The virtual machine list makes it easy to launch a virtual machine or to connect to the virtual machine's configuration file in order to make changes in the configuration.

VMware Authorization Service — The service VMware GSX Server employs to authenticate users. The process is called `vmware-authd` on Linux hosts.

VMware guest operating system service — One of the components installed with VMware Tools that performs various duties in the guest operating system, like executing commands in the virtual machine, gracefully shutting down and resetting a virtual machine, sending a heartbeat to VMware GSX Server, synchronizing the time of the guest operating system with the host operating system and passing strings from the host operating system to the guest operating system.

VMware Management Interface — A browser-based tool that allows you to control (start, suspend, resume, reset and stop) and monitor virtual machines and the server on which they run.

VMware Registration Service — The service VMware GSX Server employs for managing connections to virtual machines and the management interface. This process is known as `vmware-serverd` on Linux hosts.

VMware Tools — A suite of utilities that enhances the performance of your guest operating system. VMware Tools includes the SVGA driver, a mouse driver for some guest operating systems and the VMware Tools control panel.

Index

Symbols

.cfg 94

.dsk 85, 94, 376

.pln 85, 94

.raw 85, 94

.REDO 86, 95

.std 47, 86, 95, 376

.vmdk 47, 76, 85, 94, 97, 243, 246, 376

.vmss 47, 86, 95, 376

.vmx 85

A

Access
  to raw disks 396, 398

Apache server
  and the VMware Management Interface 183

ASCII characters 161, 177

Authentication 148–155

Autofit 239

Automatic bridging 417

B

BIOS
  provided in virtual machine 24

Bridge 406

Bridge mapping 418

Bridged networking 408
  configuring options 417
  when creating a virtual machine 90, 104

BSD
  installing guest operating system 355

Build number 127

C

CD-ROM image file 24

Chip set
  provided in virtual machine 24

Clustering 546
  applications 547
  cluster in a box 548
  configuring virtual machines 549
  multinode Network Load Balancing cluster 558
  Network Load Balancing 557
  software 547
  two-node clusters 550

Color
  screen colors in a virtual machine 471

COM5, COM6 devices in guest 274, 278

Command line 240

Commit 369

Configuration Editor 228, 368

Configuration files
  and other VMware products 147
  permissions 147

Configuration Wizard 97, 365

Copy 223

Core files 34

CPU idle program 280

Ctrl-Alt 210

Cut 223

D

Default directories 43, 53

Defragmenting disks 374–376

Devices
  adding, configuring and removing 237
  connecting and disconnecting 239
  disconnecting from USB controller 516
  provided in virtual machine 24
  USB 513

DHCP 410, 411, 423, 429, 459
  configuring on a Linux host 424
  configuring on a Windows host 424

DHCP server 407

dhcpd 429

Dial-up connection 428

Direct memory access
  See DMA

Discard 369

Disk files 372

Disk modes 228
  nonpersistent 228, 231, 370
  persistent 228, 368
  undoable 228

Disk Types
  See Disks

Disks
  See also Virtual disk
  adding virtual disks 377, 380
  defragmenting 374–376
  plain 367, 388
  raw 366
  renaming virtual disks 47, 376
  shrinking 221, 374–376
  undoable 369
  virtual 365

DMA
  and disk performance 402, 536

DNS 459

Docking station 439

DOS
  installing guest operating system 280

DOSIDLE.EXE 280

Drives
  available in virtual machine 24

dskrename.exe 376

Dynamic domain name service 430

E

EMM386.EXE 279

F

Firewall 463

Floppy
  drives in virtual machine 25
  image file 25, 394

FreeBSD
  installing guest operating system 355
  sample configuration file 357
  VMware Tools for 118

FTP 459

Full screen mode 222
  switching between virtual machines 222

G

gated 429

Generic SCSI 517–520

Guest operating system
  defined 17
  installing 107, 251
  supported 27, 254
  unsupported 255

H

Headless 187, 194, 195

Hints 220

Host computer
  system requirements 18

Host operating system
  defined 17

Host-only adapter 406
  disabling 420
  removing 420

Host-only networking 411
  dhcpd 429
  enabling on Linux host 55
  gated 429
  routed 429
  selecting IP addresses 423
  when creating a virtual machine 104

Hot-keys 210
  preferences for a console 210–212

I

ICMP 459

IDE
  drives in virtual machine 24

Image file
  floppy 25, 394
  ISO 24, 392, 393, 394

Input 208

Install
  default directories 43, 53
  FreeBSD guest 355
  guest operating system 107, 251
  guest operating system on raw disk 396
  Mandrake Linux guest 282, 284, 286, 288
  MS-DOS guest 280
  NetWare 5.1 guest 347
  NetWare 6.0 guest 343
  NetWare 6.5 guest 343
  NetWare guest 351
  on Linux host 50
  on Windows host 40
  Red Hat Linux guest 291, 294, 298, 301, 304, 307, 310
  server software 38–56
  software in a virtual machine 222
  SuSE Linux guest 312, 314, 316, 319, 322, 324, 326, 328, 330, 332, 334, 336, 338
  Turbolinux guest 339, 341
  VmCOM API 65–66
  VmPerl API 67
  VMware GSX Server 37
  VMware Management Interface software 57–58
  VMware Remote Console software 63–64
  VMware Tools 113, 193
  Windows 2000 guest 263
  Windows 3.1x guest 280
  Windows 95 guest 275
  Windows 98 guest 272
  Windows Me guest 270
  Windows NT guest 266
  Windows XP guest 260

Instant restore 197

Internationalization 18

Internet connection sharing 411

Internet Explorer 6.0
  and management interface 61

Iomega
  parallel port Zip drives 491

IP address
  assigning 426
  in virtual machine 90

IP forwarding 427, 428

ISO image file 24, 392, 393, 394

K

Keep 369

Kernel
  reconfiguring GSX Server after Linux kernel upgrade 55

Key code
  mapping 506

Keyboard 207
  key code mapping 506
  keysym 505
  keysym mapping 506
  mapping on a Linux host 504–512
  scan code 504
  table of V-scan codes 507
  USB 516
  V-scan code 504

Keysym 505
  mapping 506

L

Leaks
  IP packets in a virtual machine 428
  IP packets in host-only network 427

Linux
  creating virtual machines on Linux host 94

Linux *(continued)*
installing on Linux host 50
supported guest operating systems 27, 254
uninstalling on Linux host 70
upgrading on Linux host 78
VMware Tools for 117
Local console 194
See also VMware Remote Console
and full screen mode 222
closing 217
hot-key preferences 210–212
input preferences 207–210
memory preferences 214–216
permissions 191
priority preferences 212–213
resume options 194
special power options 195
starting on a Linux host
starting on a Windows host 188
using 191
workspace preferences 216
Localization 18
Lock files 373
Log files 34, 86, 94

M

MAC address 428
assigning manually 428
Mandrake Linux
installing guest operating system 282, 284, 286, 288
Master installer
on Windows host 40
Memory 529
available in virtual machine 24
more than 1GB on a Linux host 532
preferences 214–216
reserved memory 530
virtual machine memory size 529
Migrate
upgrading virtual disks 114
virtual machine 75, 78
Migrating
disks in undoable mode 248
virtual machines 246
MIME type, setting 183
Mouse 207
on a Linux host with XFree86 3.3.3.0 474
USB 516
MS-DOS
installing guest operating system 280
supported guest operating systems 27

N

NAT 409, 458–467
advanced configuration 461
and DHCP 459
and DNS 459
and the host computer 458
external access from a NAT network 459
ICMP 459
ping 459
sample configuration file for Windows host 466
selecting IP addresses 423
when creating a virtual machine 90, 104
NAT adapter
disabling 420
removing 420
NAT device 407
NAT service
disabling 421
removing 421
nat.conf 461, 466
NetWare
installing guest operating system 351
NetWare 5.1
installing guest operating system 347
NetWare 6.0
installing guest operating system 343
NetWare 6.5
installing guest operating system 343
Network
adding and modifying virtual network adapters 415
bridge 406
bridged networking 408
changing the configuration 415
common configurations 408
components 406
configuring 404
configuring bridged networking options 417
custom configurations 412
DHCP server 407
enabling host-only networking on Linux host 55
hardware address 428
host-only adapter 406
host-only networking 411
host-only subnet 423
in Windows 2000 guest 264
in Windows 95 guest 276, 277, 278
in Windows 98 guest 273
in Windows Me guest 271
in Windows NT guest 267
in Windows Server 2003 guest 258
in Windows XP guest 261
IP packet leaks 427
MAC address 428
NAT 409
NAT device 407
NAT subnet 423
promiscuous mode on a Linux host 457
routing between two host-only networks 452
routing on a Linux host 429
second bridged network on a Linux host 446
switch 406
switching adapters on a Windows host 439
teamed NICs 445
two host-only networks 447

Network *(continued)*
Virtual switch 406
vlance driver 258, 261, 264, 415, 441
vmxnet driver 258, 261, 264, 415, 441
Network adapter 407
Network address translation
See NAT
Network Load Balancing
clustering 557
New Virtual Machine Wizard 87, 365
Newsgroups 33
Nonpersistent mode 228, 231, 370
nvram 85, 236

O

Operating system
supported guest 27, 254
supported Linux host 20
supported Windows host 20
unsupported guest 255

P

Packet filtering 428
Parallel ports 484–491
and Iomega Zip drives 491
and the host computer's BIOS 488
and the Linux kernel 95, 484
bidirectional 484
configuring on a Linux host 488
devices you can use 491
installing in virtual machines 485
unidirectional 484
Passwords
Samba password file 435
Paste 223
Performance
CD-ROM drive polling 524
debugging mode 524
disk options 525
guest operating system selection 523
installing applications in a guest 526
Linux guest 538
memory settings 523
memory usage 529
process scheduling on a Windows host 527
remote disk access 526
system timer on a Linux host 528
using full screen mode on a Linux host 528
Windows 2000 guest 534
Windows 95 and Windows 98 guests 536
Permissions 147, 148–155
and registering virtual machines 152
and running virtual machines 86, 95
defaults 153
local console 191
VMware Management Interface 161
VMware Remote Console 191
Persistent mode 228, 368
Physical disk
See Raw disk
Ping 459
Plain disk 85, 94, 367, 388
creating 388
plain disk 92
Power buttons
for a virtual machine 192
Power on options 194
Process scheduler 212
Processor
provided in virtual machine 24
Product activation
Windows Server 2003 258
Windows XP 262
Promiscuous mode 457

R

Raw disk 366
adding 384
installing guest operating system on 396
Real time clock
requirement on Linux host 95
Red Hat Linux
installing guest operating system 291, 294, 298, 301, 304, 307, 310
Redo log 86, 95, 369, 371, 372
location 369, 371
Registering virtual machines 145–147
Registration 34
Remote management 144
VMware Remote Console 144
VMware Scripting APIs 144
vmware-cmd 144
Reserved memory 214
Resume 229
repeatable 231
routed 429
Routing
for a host-only network on a Linux host 429

S

Samba
already running on a Linux host 436
and file sharing on a Linux host 431
and printer sharing 432
on both bridged and host-only networks 436
password file 435
running two Samba servers 437
sample configuration file 432, 433, 437
Scan code 504
Screen shot
capturing 239

Scripts
running during power state changes 122
VMware Tools and 125, 129
SCSI
adding a generic SCSI device 518, 519
avoiding concurrent access on a Linux host 519
connecting to generic SCSI devices 517
devices in virtual machine 25
driver for Windows Server 2003 guest 517
driver for Windows XP guest 517
generic SCSI on a Windows host 518, 519
installing driver in Windows NT guest 517
permissions for a generic SCSI device on a Linux host 519
SCSI reservation
and clustering 541
enabling 543
issues to consider 544
plain disks 388, 541
sharing SCSI disks 541
support 542
Security 148–155
Security settings 182
Serial number 40, 87
Serial ports 492–503
between two virtual machines 497
connecting host application to virtual machine 495
connecting to a serial port on the host 492
debugging between virtual machines 503
debugging in a virtual from the host 501
improving CPU performance 500
input connection speed 500
installing and using 492–503
session lengths
VMware Management Interface 163
Settings 208
Shrinking disks 374–376
Shut down
a virtual machine 235
smb.conf 432, 433, 437
SMBIOS
modifying the UUID 158
Sound
configuring 475
in a Linux guest 478
in a Windows 2000 guest 263, 477
in a Windows 95 guest 277
in a Windows 95 or Windows 98 guest 478
in a Windows 98 guest 272
in a Windows Me guest 270
in a Windows NT guest 267, 477
in a Windows Server 2003 guest 258
in a Windows XP guest 261
in a Windows XP or Windows Server 2003 guest 476
on a Linux host 476
on a Windows host 475
supported and unsupported capabilities 479
Specifications
virtual machine platform 24
SSL 155
SuSE Linux
installing guest operating system 312, 314, 316, 319, 322, 324, 326, 328, 330, 332, 334, 336, 338
Suspend 229, 235
Switch 406
System requirements 18
host server 18
remote workstation 22

T

Teamed network interface cards 445
Technical support 33
Telnet 459
Text
cutting, copying and pasting 223
Token Ring 410, 411
Turbolinux
installing guest operating system 339, 341

U

Undoable mode 228
commit changes 369
discard changes 369
keep changes 369
migrating 248
Uninstall
host-only adapter 420
NAT adapter 420
NAT service 421
on Linux host 70
on Windows host 68
Upgrade
from GSX Server 1 72
on Linux host 78
on Windows host 75
virtual disks 114
virtual hardware 80
virtual machine 75, 78
VMware GSX Server 71
USB 513–516
connecting devices 513
control of devices by host and guest 515
disconnecting devices 516
enabling and disabling the controller 513
keyboard and mouse 516
notes on supported device types 513
on a Linux host 514
on a Windows host 514
UUID
modifying 158, 244, 245, 247

V

Video
  resolution on a Linux host 473
  resolution switching on a Linux host 474
Virtual disk 365
  See also Disks
  location 87
  migrating 114
  renaming 376
  shrinking 128, 131
  size 87, 91, 101, 378, 379
Virtual hardware
  upgrading 80
Virtual machine
  upgrading 75, 78
  window size 239
Virtual machines
  capturing screen shot of 239
  constituent files 85, 94
  creating 83
  creating on Linux host 94
  creating on Windows host 85
  installing software in 222
  instant restore 197
  location 99, 216
  migrating 246
  platform specifications 24
  power buttons 192
  power on from local console 194
  registering on Linux hosts 147
  registering on Windows hosts 146
  resuming 229
  running headless 187, 194, 195
  running off CD-ROM/DVD-ROM discs 235
  settings 207–216
  shutting down 235
  special power options 195
  suspending 229, 235
Virtual switch 406
vlance driver 415
VmCOM Scripting API 65
vmnet1.conf 430
VMnet8 458
vmnetdhcp.conf 425
vmnetnat.conf 461
VmPerl Scripting API 65
VMware Authorization Service 149
VMware guest operating system service
  executing commands on halt or reboot 137
  passing information between the guest and a VMware Scripting API script 140
  passing strings from the host 137
  time synchronization 136
  VMware Tools 136–140
VMware Management Interface 161–184
  and Apache server 183
  ASCII characters 161, 177
  attaching VMware Remote Console 166
  browsers required 163
  changing virtual machine power state 168
  configuring for Windows systems 61
  connected users 173
  controls 166–170
  creating a new virtual machine 177–180
  deleting a virtual machine 181
  event log 174
  host status monitor 165
  launching remote console 61
  launching remote consoles 63
  logging in 163
  logging out 182
  permissions 161
  proxy servers 62
  refresh rate 162
  remote management 144
  security settings 182
  session lengths 163
  setting remote console MIME type 183
  timeout 182
  virtual machine details 171
  virtual machine hardware 172
  virtual machine menu 167
VMware Remote Console 187
  See also Local console
  attaching from VMware Management Interface 166
  changing port number 198
  closing 217
  downloading from VMware Management Interface 202
  hot-key preferences 210–212
  input preferences 207–210
  installation 63–64
  launching from management interface 61
  memory preferences 214–216
  permissions 191
  priority preferences 212–213
  remote management 144
  securing connections 155
  setting a MIME type 183
  special power options 195
  starting on a Linux host 190
  starting on a Windows host 189
  uninstalling 201
  upgrading 201
  using 191
  workspace preferences 216
  X server 58
VMware Remote Console banner 198
VMware Scripting APIs 144
  installing 65
VMware Tools
  build number 127
  choosing scripts 125, 129
  configuring 124
  for FreeBSD guests 118

VMware Tools *(continued)*
for Linux guests 117
for Windows guests 113
installing 113, 193
running scripts during power state changes 122
status 221
VMware guest operating system service 136–140
vmware.log 86, 94
vmware-cmd 144
vmware-config.pl 55
vmxnet driver 415
V-scan code 504
table of codes 507

W

Window size 239
Windows
creating virtual machines on Windows host 85
installing on Windows host 40
supported guest operating systems 27, 254
uninstalling on Windows host 68
upgrading on Windows host 75
VMware Tools for 113
Windows 2000
installing guest operating system 107, 263
vmxnet network driver 264
Windows 3.1x
installing guest operating system 280
Windows 95
installing guest operating system 275
upgrading guest 81
Windows 98
installing guest operating system 272
upgrading guest 81
Windows Event Log 175
Windows Me
installing guest operating system 270
upgrading guest 80
Windows NT
installing guest operating system 266
installing SCSI driver in guest 517
Windows operating system
installing Scripting APIs on 65–67
Windows Server 2003
installing guest operating system 257
product activation 258
SCSI driver for guest 517
vmxnet network driver 258
Windows XP
installing guest operating system 260
product activation 262
SCSI driver for guest 517
vmxnet network driver 261
Wireless LAN adapter 410
Write caching 380, 382, 387, 391

X

X server 58
and keyboard mapping 504
configuring 473
required on Linux host 22
XF86Config 473
XFree86
and keyboard mapping 504
configuring 473
mouse problems in version 3.3.3.0 474
required on Linux host 22

Z

Zip drives
on a parallel port 491